2008

DEFACING THE ‘BOOK: EXAMINING INFORMATION REVELATION, INTERNET PRIVACY CONCERNS AND PRIVACY PROTECTION IN FACEBOOK

Alyson L. Young

DEFACING THE 'BOOK:
EXAMINING INFORMATION REVELATION, INTERNET PRIVACY CONCERNS AND PRIVACY PROTECTION IN FACEBOOK

(Spine title: Defacing the 'Book)

(Thesis format: Monograph)

by

Alyson L. Young

Graduate Program in Media Studies

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts

School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

Abstract

The focus of much research on social network sites (SNSs) has been on the amount and types of information revealed, the relatively open nature of the information, and the apparent lack of controls employed by users. The aim of the present study was to expand the research in this area by identifying the factors that influence information revelation and privacy protection on Facebook, as well as to examine the strategies developed by students to protect themselves against privacy threats. A mixed-methods data collection approach was employed that included a questionnaire, semi-structured interviews and profile analyses. Findings show that students manage their Internet privacy concerns by withholding personal information and address their concerns about unwanted audiences by altering the visibility of their information from within the site. The findings provide insight into students' motivations for information revelation on Facebook and the ways in which they negotiate privacy on the site.

Keywords: social network sites, Facebook, information revelation, privacy, Internet privacy, privacy protection, university students

Acknowledgements

I am grateful to all the people who made this thesis possible. Foremost, I would like to thank my supervisor and mentor, Dr. Anabel Quan-Haase, for her encouragement, enthusiasm and dedication. She encouraged me to learn as much as possible and was always available when I needed her help or advice (especially when analyzing statistical data). Without her tolerance and support, this project would have never come to fruition. I would also like to thank my second reader, Dr. Jacquie Burkell, for her assistance with proposals, instruments and drafts. Dr. Burkell's knowledge of privacy made her a valuable source of information.

I would also like to acknowledge the support of my family and friends. Without them the process of writing this thesis would have been unbearable. Thanks to my mom, dad, and stepparents, Pam and Bill, for believing in me and providing me with constant support and encouragement. Many thanks to my brother Matthew and stepsister Victoria for being wonderful siblings and incredible friends – I admire their passion for life, ambition, and drive to excel in everything they do. Also, warm thanks to my grandparents for always being there for me and for providing me with unconditional love and support. Many thanks to Aaron Tallon for providing me with an ear to bounce off ideas and for his constant support and encouragement in times of frustration and stress. To all my friends at UWO, thank you for making my Masters an enjoyable and rewarding experience.

I would like to dedicate this thesis to my grandmother (Granny) Phyllis Stratton who passed away in September 2005. I marvel at her ability to always look at the bright side of life and her knack for adapting to new and unfamiliar situations. Her strength and independence are traits that I strive towards everyday of my life.

Table of Contents

List of Figures

List of Tables

List of Appendices

CHAPTER 1
INTRODUCTION

1.1. BACKGROUND OF THE STUDY

Over the past few years, social network sites[1] (SNSs), such as MySpace, Friendster and Facebook, have rapidly increased in popularity. Indeed, research has shown that approximately 80 to 90 percent of undergraduate university students are active participants (Strater and Richter 2007). The popularity of these sites stems, in large part, from the fact that users are able to converse with their friends and peers, share digital cultural artifacts and ideas, and connect to vast networks of people (boyd and Heer 2006). Moreover, through the construction of a profile users are able to signal aspects of their personality, which assists in identity formation and performance (boyd in press; Laraqui 2007).

These sites, however, have received significant criticism from the media, scholars and privacy advocates who argue that the disclosure of personal information on SNSs has negative consequences and privacy risks for users. Several media reports have documented the risks associated with revealing personal information on SNSs, outlining three general areas of concern for users. First, they contend that university officials have started using SNSs to locate and discipline university code violators for engaging in illegal activities, such as underage drinking, or acting in a manner that violates university policy (Augustinas 2005; Brown 2008a; Brown 2008b; Jones 2007; Klein 2006; Panja 2007). Second, they argue that unwanted audiences, such as sexual predators, may use SNS profiles and the information disclosed within to harass or stalk users (Buckman 2005). Third, they suggest that employers have begun accessing SNS profiles in order to assess candidates' suitability for employment with their organization (*CBS Evening News* 2006). These three areas of concern have been used to draw attention to the risks

[1] In the context of the present study, the term social network sites (SNSs) is used to describe online spaces, which allow users to create a profile and link that profile to other users to create a personal network. While the terms social networking (Web)sites and social network sites have been used interchangeably in the current literature, the former focuses on expanding one's social network (i.e., meeting new people), whereas the latter refers specifically to transferring one's already established social network to an online space. Although network expansion is possible on these sites, it is not a primary objective of users. Therefore, the term social network sites or SNSs will be used in the context of the present study.

associated with disclosing personal information on SNSs, indicating that users should be cautious about the amount and types of information that they chose to reveal on these sites.

Aside from the concerns raised by the media, much of the current research on privacy in SNSs has suggested that the disclosure of personal information on SNSs may have implications for users. For example, in her article examining social networking privacy issues in the United States, Susan B. Barnes contends "that because schools, college admissions officers, and future employers are checking [SNSs], personal information and pictures revealed online can directly influence a student's education, employment and financial future" (2006, under "Privacy"). Similarly, Gross and Acquisti (2005) argue that in disclosing personal information on Facebook users effectively place themselves at a greater risk for cyber and physical stalking, identity theft and surveillance.

Despite these concerns, research has consistently demonstrated that users continue to disclose large quantities of personal information on SNSs and often use accurate personal information on their profiles. Some evidence exists suggesting that different factors are likely to influence information revelation on SNSs and on the Internet more generally. First, Lampe, Ellison and Steinfield (2007) provided evidence showing a correlation between the disclosure of personal information on Facebook and users' personal network size. Their work examined how aspects of signaling theory, common ground theory, and transaction cost theory can be used to assist in understanding why certain profile fields are likely to predict friendship articulation on the site. Their results showed that populating certain profile fields, such as 'about me', interests and favorites, led to larger social networks on Facebook. Thus, their results suggest that the disclosure of personal information on SNSs encourages connections and the articulation of relationships between users.

Second, the literature on privacy online has documented the presence of a 'nothing to hide, nothing to fear' attitude among a subsection of Internet users (Marx 1999; Viseu, Clement, and Aspinall 2003). This attitude, according to Marx (1999), is premised on the assumption that only the individuals who have done something wrong have something to hide. Viseu, Clement and Aspinall (2003) showed that Internet users who possess this attitude, and who have not experienced any negative consequences as a result of their use of the Internet in the past, were more apt to provide truthful and accurate information online. Thus, for this group of Internet users, privacy only becomes a concern once it has been lost or breached.

Third, research has suggested that the benefits of disclosing personal information online may outweigh the potential privacy risks and negative social consequences that these disclosures may produce. In a report released by the Pew Internet and American Life Project (2000) on trust and privacy online, for instance, researchers found that 64 percent of Internet users are willing to provide personal information, such as their name and email address, in order to use a Web site even though they do not think that Internet companies should be allowed to track their online behavior without their consent. Thus, research suggests that users who perceive the benefits of disclosing personal information to be greater than the potential privacy risks will reveal more personally-identifiable information online.

All three lines of research discussed above provide evidence suggesting that various factors are likely to influence information revelation on SNSs. In the context of the present study, information revelation refers to the disclosure of personal information, such as name, age, birth date, email address, sexual orientation, relationship status, and physical address. While the terms self-disclosure and information revelation have been used interchangeably in the current literature on SNSs, the former focuses primarily on the disclosure of one's thoughts, emotions, aspirations, goals, likes and dislikes, whereas the latter examines a wider range and diversity of information types, such as those discussed above. As such, the term information revelation is used in the context of the present study to examine the disclosure of personal information on SNSs.

Examining information revelation on SNSs is relevant because SNSs are being used and adopted by large numbers of individuals who disclose considerable amounts and types of personal information. Given the privacy risks and negative social consequences associated with the disclosure of personally-identifiable information on these sites, it is important to understand the reasons why users chose to reveal personal information. However, few studies have specifically examined users' motivations for revealing personal information on SNSs (boyd in press; Tufekci 2008). Such an examination is relevant because various factors are likely to influence users' information revelation practices on these sites.

In addition to examining the factors that influence users' information revelation on SNSs, an examination of the strategies that users have developed to protect themselves against privacy threats and the factors influencing their privacy protection practices is also important. Such an examination is relevant because it might provide further insight into the reasons why users willingly disclose personal and private information on these sites. For example, use of a site's privacy settings, such as altering one's profile visibility to 'only friends', may influence users to disclose more information because they may believe that their information is private and inaccessible by unwanted audiences. Furthermore, while privacy protection on SNSs has been investigated, few studies have engaged directly with users to better understand how they negotiate privacy while using these sites. Much of the current research on privacy in SNSs has examined privacy protection by measuring the presence or absence of privacy controls. However, it seems likely that users will have developed additional strategies, such as the exclusion of certain types of personal information, in order to protect themselves.

1.2. PURPOSE OF THE STUDY

Although a body of literature has started to emerge in this area, the general focus has been on the amount and types of personal information users indicate on their profiles, the relatively open nature of the information disclosed on these sites, and the apparent lack of controls employed by users to protect themselves against privacy threats (Govani and Pashley 2006; Gross and Acquisti 2005). What has not received sufficient attention are the factors that influence information revelation and privacy protection on SNSs and the strategies that users have developed to protect themselves. The motivation to conduct an analysis of information revelation and privacy protection in SNSs is the idea that an examination of the information indicated on the users' profile, as well as whether they employ the site's privacy controls, cannot provide a comprehensive understanding of the information revelation and privacy protection practices, habits and behaviors of users. The aim of this study therefore was to identify the factors that influence information revelation and privacy protection on Facebook, as well as the strategies developed by students to protect themselves against privacy threats, in order to expand the research in this area.

1.3. RESEARCH QUESTIONS

(1) What influences undergraduate students' information revelation on Facebook?

The present study investigated the factors that influence undergraduate students' decision to either reveal or conceal personal information on Facebook. Previous research on SNSs and privacy has consistently demonstrated that users tend to disclose substantial amounts and types of private information and often use accurate private information on their profiles (Acquisti and Gross 2006; Barnes 2006; Govani and Pashley 2006; Gross and Acquisti 2005). However, there is little understanding about the reasons users willingly disclose personal information on SNSs. Tufekci (2008) conducted a large-scale survey of undergraduate students to investigate factors that influence information revelation in SNSs. Important factors identified were future audiences, general privacy concerns, and gender. To further investigate information revelation on SNSs, a first step was to examine what information users reveal on their profiles and to see if their information revelation practices are consistent with previous findings. Second, I continued Tufekci's line of inquiry and asked students directly in an interview about what information they have disclosed. This provided a more comprehensive understanding of the factors that influence undergraduate students to reveal personal information on their profiles than an examination of their information alone.

(2) What factors influence privacy protection in Facebook and what strategies have undergraduate students developed to protect themselves against privacy threats?

The present study also investigated the factors influencing privacy protection in Facebook and the strategies developed by students to protect themselves against privacy threats. In her examination of audience and disclosure regulation on MySpace and Facebook, for example, Tufekci (2008) found that concern about unwanted audiences accessing students' profiles influenced students to use protective measures, such as altering the visibility of their profile to 'only friends' on Facebook and using nicknames or monikers in place of real names on MySpace. These results suggest that various factors are likely to influence privacy protection on Facebook. Research question 2 examines what factors influence privacy protection.

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. For example, 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. By contrast, in two separate studies conducted at Carnegie Mellon University (CMU), 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. Therefore, the present study expanded the current research on privacy in SNSs by examining the strategies developed by undergraduate students to protect themselves against privacy threats.

1.4. RESEARCH APPROACH

To investigate information revelation and privacy protection on Facebook, a mixed methods approach to research is ideal because it allows the researcher "to use all the tools of data collection available rather than being restricted to the types of data collection typically associated with qualitative research or quantitative research" (Creswell and Clark 2007, 9). In this way, a mixed methods research approach enables the researcher to use the strengths of one method to offset the weaknesses of another method (Axinn and Pearce 2006). In the present study, questionnaires were used to collect data on the amount and types of information indicated on respondents' profile, respondents' level of concern for Internet privacy and the possibility of unwanted audiences accessing their profile, and the mechanisms employed by respondents to protect themselves against privacy threats and negative social consequences while using the service. Given the weakness of quantitative research in providing an in-depth, first-hand account of respondents views and perspectives, semi-structured interviews and profile analyses were used to gain a better understanding of the reasons undergraduate university students reveal personal information on their profiles, as well as to further understand the strategies that undergraduate university students have developed to negotiate privacy on Facebook. In addition, the profile analyses provided visual confirmation concerning the information disclosed and the privacy settings activated by the respondents. The qualitative data were used to expand and explain the quantitative results.

1.5. SIGNIFICANCE OF THE STUDY

This study examined undergraduate students' information revelation and privacy protection on Facebook. While a body of literature has started to emerge in the area of privacy in SNSs, little is known about students' motivations for information revelation and privacy protection on these sites. By identifying the factors of information revelation and privacy protection, this study adds to the current research on privacy in SNSs by providing insight into students' reasons for information revelation on Facebook and the ways in which they negotiate privacy on the site. Moreover, this study also provides insight into students' privacy protection by examining two levels of profile visibility: 1) outside profile visibility, which focuses on the extent to which students' profiles are visible by other Facebook users and 2) inside profile visibility, which refers to the visibility of students' information from within the site. Currently, research on privacy in Facebook has examined profile visibility by looking at either outside profile visibility (Gross and Acquisti 2005; Tufecki 2008) or inside profile visibility (Govani and Pashely 2006). However, no research to date has examined both levels of profile visibility within a single study. The present study therefore adds to the current research on privacy in Facebook by examining inside and outside profile visibility within the same study.

This study is also unique in that it examines information revelation and privacy protection following Facebook's decision to allow general audiences to create profiles on the site. Prior to September 2006, individuals required an email address that verified their affiliation with a specific university/college, corporation or high school. Each university/college, corporation and high school was subsequently represented by its own network, which, by default, allowed individuals within the same network to access each other's profiles. This, in turn, contributed to users' perceptions of Facebook as an intimate and private community (boyd and Ellison 2007). At present, much of the research on privacy in Facebook has examined users' information revelation and privacy protection practices prior to Facebook opening the site to the general public (Acquisti and Gross 2006; Govani and Pashley 2006; Gross and Acquisti 2005; Tufecki 2008). Thus, it seems likely that the results of the past studies may not reflect students' existing information revelation and privacy protection behaviors. As Tufekci (2008) notes, in allowing anyone to create a profile on Facebook, students' perceptions of Facebook as a 'walled garden' may be altered, thus affecting their behavior on the site. The present study therefore provides new insight into students' behaviors by examining their information revelation and privacy protection practices following Facebook's decision to open the site to everyone.

Furthermore, considering that researchers have often studied privacy in SNSs by downloading profiles in order to analyze the amount and types of information that users disclose (Acquisti and Gross 2006; Govani and Pashley 2006; Gross and Acquisti 2005), it is useful to develop a new approach. The present study proposed to examine Facebook profiles in the presence of students. The Facebook profile analyses were conducted during the interview phase, which enabled me to validate the data provided in the interviews and afforded participants the opportunity to discuss their reasons for information revelation on Facebook, as well as their privacy protection strategies. Furthermore, the profile analyses showed that students are often unaware or have forgotten what information they have disclosed and what privacy settings they have activated. The findings of this study therefore provide an alternative approach for researchers to examine SNS profiles in order to better understand the information revelation and privacy protection strategies and practices of users.

The findings of this study also have implications for university students. Identifying the possible consequences and privacy risks associated with the disclosure of personal information on Facebook, as well as the privacy protection options available, may assist in providing a guideline for students to use Facebook in the future. Currently, I am helping to develop these guidelines (see Appendix H, p. 106) for the University of Western Ontario to address the concerns that arose from the York University case, in which a student faced expulsion for using Facebook to run an online study group. These guidelines will inform students of the issues that can happen within privacy and describe the privacy options available to support their privacy concerns and objectives. Thus, the goal of these guidelines is to assist students in making informed decisions about their information revelation practices and privacy protection options.

CHAPTER 2
LITERATURE REVIEW

This chapter consists of a literature review to provide theoretical background for the study. The chapter commences by reviewing various theories and definitions of privacy to provide a basis for examining privacy within the context of social network sites (SNSs). The chapter continues with the literature on privacy online, focusing specifically on how the Internet has altered the way we perceive and practice privacy. Then, a historical overview of SNSs is provided. From here, privacy in SNSs is discussed. The focus is on the perceived privacy risks and negative social consequences associated with information revelation on SNSs. Then, the possible reasons for information revelation on the Internet and on SNSs are examined to highlight some of the factors that might influence users to willfully disclose personally-identifiable information on SNSs despite the perceived privacy risks. Finally, the chapter concludes with an examination of the strategies users have developed to protect themselves against privacy threats.

2.1. PRIVACY

2.1.1. Definitions, Properties, and Functions

Privacy is a fluid and far-reaching concept, which has been defined in several different ways and which varies depending on situational and contextual factors. This section examines the key theories and literature on privacy to illustrate the fluidity of the concept and to arrive at a definition suitable to guide the study.

Margulis (2003b) has identified two perspectives of privacy: the sociopolitical and the psychological perspectives. From a sociopolitical perspective, privacy refers to a core of fundamental rights and freedoms afforded individuals in a liberal democratic society, including freedom of expression, freedom of thought, freedom from unwarranted police and government interference, and freedom for political expression and criticism (Margulis 2003b; Westin 1967). These properties, while important for the proper functioning and development of any political democracy, are not as applicable to the current study of privacy in SNSs and therefore will not be treated in more detail in this review.

Within the sociopolitical dimension of privacy exists the concept of informational privacy, which focuses on individuals' control over personal data, including "what information about [oneself] should be known to others, ... when such information will be obtained and what uses will be made of it by others" (Westin 2003, 431). This aspect of the sociopolitical perspective directly reflects the pragmatic concerns associated with privacy in SNSs, such as surveillance and identity theft, and therefore will be discussed in detail in this review.

Informational privacy – that is, the protection or control over one's personal information – is by far one of the most frequently discussed aspects of privacy (Goldie 2006), and has become especially relevant as a result of technological advancements in electronic information collection and storage (Goldie 2006; Westin 1972). In *Databanks in a Free Society* (1972), for instance, Alan Westin describes how the automation of 'record-keeping looms' in the 1960's made it possible for large organizations to move information about individuals from the filing cabinet to the computer. While supporters of the high technology society viewed this shift as beneficial, "since it promised to enable organizational evaluators to obtain timely and complete information with which to make truly informed decisions about individuals" (Westin 1972, 3), others feared that the incredible speed at which data could be processed, the increased storage capacity, and the rapid data communication that computer systems permitted would inevitably lead to the collection, consolidation and exchange of larger amounts of information about individuals than was previously possible in the pre-computer era (Westin 1972). "Such a trend," Westin contends, "was seen as threatening the boundaries of personal privacy and confidentiality that had evolved out of a combination of technological limitations and civic-liberties rules in precomputer America" (1972, 4).

From a more practical standpoint, informational privacy has come to center on the argument that much information about oneself "need not be available for public perusal" (DeCew 1997, 75). Accordingly, information regarding one's financial situation, lifestyle choices and medical history may be perceived by certain individuals to be information that need not be disclosed to others and in need of more rigorous protection than other (less personal) types of information (DeCew 1997; Goldie 2006). Goldie (2006), for instance, provides the example of human resources departments' use of Social Insurance Numbers to pay employees and take care of tax-related issues. However, she contends that the mere fact that human resource departments possess this information does not give them the right to share the information with others without the individual's knowledge or consent, or to use the information for additional purposes, such as to investigate an individual's credit history or recent financial transactions (138). In this way, informational privacy concerns center around the threat of information being used or appropriated "to pressure or embarrass an individual, to damage an individual's credibility or economic status, and so on" (Goldie 2006, 138; see also DeCew 1997, 75). In other words, it is the potential to harm an individual with the possession of their personal and private information that is the greatest threat associated with informational privacy. For example, an individual could be refused employment if information regarding her previous drug use was to become known by potential employers. Informational privacy protection therefore guards individuals against intrusions as well as the threat of intrusions. It also affords individuals opportunities to decide who has access to their personal information and how the information will be used and for what purposes (DeCew 1997; Goldie 2006).

By contrast, privacy from a psychological perspective protects personal autonomy, which is important for the development and maintenance of the self and individuality. It provides individuals with opportunities for self-reflection/evaluation and experimentation; it supports emotional release outside of the public sphere, thereby allowing individuals to vent, make unfair or frivolous comments without public scrutiny; and, it enables individuals to decide for themselves when, to whom and to what extent personal information should be revealed to others (Westin 1967).

For Altman (1975), privacy also facilitates social interaction, which, in effect, presents us with feedback on our ability to cope with the world and, through this feedback, influences our self-definition (see also Margulis 2003b). Altman further contends that privacy should not be seen as a withdrawal process, but rather as a boundary regulation process in which accessibility is optimized along a range of "openness" and "closedness" dependant on contextual factors. The primary objective of privacy regulation, according to Altman, is to adjust and optimize one's behaviors for a given situation or event in order to achieve the desired levels of privacy (or state of "openness" or "closedness"). In this theory, desired levels of privacy are achieved through behavioral mechanisms that regulate social participation. These mechanisms include, but are not limited to, nonverbal use of the body such as adverting direct eye contact or covering the face, environmental behavior such as the use of objects to create physical barriers between the self and others, and culturally-based norms and practices. These different mechanisms operate in an integrated fashion and can be used to substitute, strengthen, or modulate one another (Altman 1975).

Altman's understanding of privacy as a dialectic and dynamic process is analogous to Arnold Simmel's (1971) discussion of privacy as an interpersonal boundary control process in which the individual regulates his or her social interactions by strategically opening and closing the self to others. Simmel elaborates:

> We need to be part of others, of intimate circles, families, communities, nations, part of humanity, and we need to be so recognized by others, to be supported by their approval for our affiliation and our likeness to them. But we also need to confirm our distinctiveness from others, to assert our individuality, to proclaim our capacity to enjoy, or even suffer, the conflicts that results from such assertions of individuality (1971, 73).

Simmel's understanding of privacy as a dialectic of forces resonates with Irvin Goffman's (1959) theory of front and back regions. In front regions, or "on-stage", the individual acts out roles in accordance with societal norms and expectations. The role that the individual assumes is context-dependent and varies depending on the situation and the audience that he or she is interacting with. It is through social participation, that is, the act of being "on-stage," that the individual learns which roles are appropriate for different contexts and audiences, and how to "impress [his or her] audience favorably, or avoid sanctions, etc." (Goffman 1959, 108). In back regions, or "off-stage," the individual "can relax; he can drop his front, forgo speaking his lines, and step out of character" (Goffman 1959, 112). It is during these periods of relaxation that the individual can reflect on his or her 'performance' and make adjustments for future performances. Privacy therefore is best viewed as the "control over transactions (interactions, communications) that regulate access to the self and that, as a consequence, reduce vulnerability and increase decisional and behavioral options" (Margulis 2003a, 415). In line with other limited-access theories of privacy, such as those put forth by Westin and Altman (see Altman 1975; Margulis 2003b; Westin 2003), this definition emphasizes the right of individuals to control and/or limit access to the self in order to achieve desired levels of privacy. From this perspective, privacy operates to protect the individual from unwanted intrusions/violations and to increase his or her opportunities for self-evaluation and individuality.

Westin (1967; 2003) also discusses how individuals seek a balance between achieving desired levels of privacy and satisfying the need for communication and disclosure. He states, "each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others" (Westin 1967, 7). This dialectic of privacy, or interplay of forces that drives people to come together and to move apart is dependent, according to Westin, on an individual's personal situation, which includes factors such as his or her family life, education, social class, and psychological constitution (2003). Furthermore, Westin contends that an individual's needs and desires are context-dependent and frequently change depending on situational events. Thus, in one instant an individual may want to be left alone, and in another may even desire or crave social participation and companionship. It is this contextual and continually shifting nature of self-censorship and self-revelation, Westin argues, that makes privacy such a complex concept and a matter of personal choice (2003).

The psychological perspective of privacy can be further understood by briefly examining DeCew's (1997) concept of expressive privacy, which Goldie (2006) summarizes as "one's ability to freely choose, act, self-express and socially interact" (139). From Goldie's perspective, the protection of one's expressive privacy – that is one's ability to control the extent to which he or she is known by chosen others – is important because it supports the development and maintenance of intimate relationships. She states: "Because intimacy is based on the self-disclosure of information, if we were unable to choose or control what information we give out or the degree to which we allow other people to know us, intimate relationships would cease to exist, and essentially everyone would know everything about everyone" (Goldie 2006, 140). In this way, expressive privacy is similar to the other theories of psychological privacy discussed above in that it affords individuals opportunities to choose and to dictate how, when and to what extent personal information should be revealed to others. This, in turn, assists in the creation of self-identity and enables individuals to enjoy a wide variety of roles and social relationships, including intimate relationships (Goldie 2006).

2.1.2. Privacy Online

The Internet has further complicated and created new challenges in the negotiation and practice of privacy. By its very nature, the Internet is "decentralized, open and interactive" (Chapman and Dhillon 2002, 76). It allows for communication, commerce, research, and the publication and disclosure of information in ways previously unavailable in offline environments. Moreover, information and conversations contained on the Web are accessible at different times and places from which they were originally typed, defying spatial and temporal constraints typically associated with offline environments. These characteristics of the Internet have led danah boyd (in press; 2007) to suggest that online environments possess four properties that fundamentally differentiate them from offline environments: persistence, searchability, replicability, and invisible audiences. These properties, according to boyd, complicate the process of identifying context and audience, which, as discussed in section 2.1.1, is important for privacy regulation. As Goffman notes, the individual tries "to segregate his audiences so that the individuals who witness him in one of his roles will not be the individuals who witness him in another of his roles" (137). However, unlike the offline world where individuals are usually able to gauge their actual and potential audience and regulate their interactions through behavioral mechanisms (see Altman 1975), in online environments "the lack of presence [or an identifiable audience] makes it difficult to know who is listening" (boyd and Heer 2006, 1). Arguably, even if an individual is able to determine his or her audience at a specific point in time, it is nearly impossible to control for future potential audiences. This is because digital expressions and conversations, unlike 'acts' in the offline world, are usually recorded and archived for posterity, for example in archive.org – an online database of archived Internet content (boyd in press, boyd 2007; O'Neil 2000; Peter 1999; Solove 2004), and search tools (such as search engines) have made it possible to locate and access digital content at a different time and place from which it was originally created. Daniel Solove, Associate Professor of Law at George Washington University Law School, concurs:

> Almost everything on the Internet is being archived ... Our online personas – captured for instance, in our web pages and online postings – are swept up as well. We are accustomed to information on the web quickly flickering in and out of existence, presenting the illusion that it is ephemeral. But little on the Internet disappears or is forgotten, even when we delete or change the information (2004, 26).

Moreover, the ease at which digital content can be copied and forwarded (boyd in press; boyd 2007; Solove 2004) means that conversations and expressions published online may not only be accessible by individuals who are temporally and spatially distant, but also by strangers who have no connection with the author. Thus, "the threats to one's privacy on the Internet can be immediate as well as future threats, because online activities can be (a) monitored by unauthorized parties and (b) logged and preserved for future access" (O'Neil 2000, 17).

The current literature on privacy online has also paid a great deal of attention to electronic commerce (e-commerce) and, more specifically, the individual's right(s) to privacy during electronic transactions. Although purchasing occurs less frequently on SNSs (i.e., Facebook offers virtual gifts for users to purchase and give to their friends), the privacy issues associated with the disclosure of personal information in e-commerce can also be applied to the study of SNSs. According to Miriam J. Metzger (2007), "Privacy is implicated in e-commerce because of the risk involved in disclosing personally-identifying information, such as email addresses or credit card information, which is required for most e-commerce transactions" (1). Drawing on data from The Digital Future Report (2005), Metzger further contends that the primary concern for online consumers is that their information will be used, without their prior knowledge or consent, for "electronic surveillance," "email solicitation" or "spam," and "data transfer," that is, the unauthorized transfer and/or sale of data to third parties (2007, 1). In line with Metzger, Thomas A. Peters (1999) suggests that while the voluntary disclosure of personal information in e-commerce is not in and of itself problematic, it may become so if the information is subsequently used in ways unintended by the discloser, or in conjunction with other information to produce a more in-depth picture of the discloser's behavioral habits (141). This has led Solove (2004) to suggest that the problem in e-commerce is that people often lack control, knowledge and participation in the collection and use of their personal data. "Without being informed about how information will be used," Solove contends, "the individual lacks the necessary knowledge to assess the implications of surrendering her personal data" (2004, 88). The European Union (EU) further supports this viewpoint. In 1998, the EU implemented the European Directive on Data Protection, which imposed three stringent requirements on the collection and use of personal information by data controllers: (1) consumers must be informed of the reasons why their personal data are being collected and must provide 'unambiguous' consent, (2) the data collected must not be transferred or used for purposes other than those stated during collection, and (3) there must be a reasonable relationship between the data collected and the purposes for which the data were collected (Goldsmith and Wu 2006, 174). Under this Directive, the EU summoned Microsoft to Brussels in 2003 to discuss the dot-Net Passport feature created in 1999 to make navigation among password protected Web sites significantly easier. The EU privacy officials were interested in learning more about Microsoft's data collection process and how they were using the information collected. The officials determined that Microsoft was collecting more information than it needed for the purposes of its program and, as result, provided Microsoft with two choices: either alter their data collection practices to adhere to EU's legal policy, or remove themselves from the European market, which constituted about a third of their sales. In the end, Microsoft elected to modify the way dot-NET Passport manages user data, which included providing users with more notice and control over how their personal data were shared (Goldsmith and Wu 2006). Thus, while the verdict is still out on how and by whom consumers' privacy rights in e-commerce should be handled, the general consensus is that online consumers require more control over their information, more knowledge about how their information will be used, and more participation in the data collection process.

2.2. SOCIAL NETWORK SITES

Currently, nowhere do such concerns over privacy become more prominent than in SNSs. Unlike e-commerce transactions, for instance, which are covered under legislation, such as PIPEDA, a large percentage of the information disclosed on SNSs is not required (such as interests, relationship status, address and sexual orientation) and therefore is not protected. Indeed, Facebook's Terms of Use Agreement stipulates that they possess the right to "use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute ... User Content for any purpose, commercial, advertising, or otherwise ... and to grant and authorize sublicenses of the foregoing" (Facebook 2007, under "Terms of Use"). Therefore, by posting information to SNS profiles, users effectively waive their rights to their information, authorizing the hosting site to use the information for a multitude of purposes. In addition, the user's psychological or expressive privacy is also at risk when using SNSs. In particular, the convergence of different contexts and audiences means that all friends, acquaintances, work associates and family members included on the user's profile has access to the same types of information. As discussed in section 2.1.2, this is problematic because individuals generally try to separate the various aspects of their identity so that the individuals who see them in one of their roles are not the same individuals who see them in another role. Therefore, the collapse of different contexts and audiences means users must be prepared to explain and account for the various aspects of their identity that they choose to display on SNSs.

The aim of the next section is to review a number of studies and reports that are relevant to the present examination of privacy and information revelation on SNSs. The section commences with a historical overview of some of the most prominent SNSs to provide a historical context for the study. The section continues with a review of the important literature on privacy in SNSs. The focus is in particular on the perceived risks and negative social consequences attributed by scholars and the media to the use of SNSs. Then, the possible factors influencing information revelation on SNSs are examined. Finally, the section concludes by investigating users' privacy protection strategies.

2.2.1. Background Information on Social Network Sites

SNSs are traditionally defined as "spaces on the Internet where users can create a profile and connect that profile to others to create a personal network" (Lenhart and Madden 2007, 1). Although electronic social networks, such as listservs, newsgroups and Internet Relay Chat (IRC), have existed in some form since the 1970's (Wellman et al.

1996), the first recognizable social network site, SixDegrees.com, was launched in 1997 (Donath and boyd 2004). Based on the adage that people are separated by six degrees, the service provided users with a space to create a profile, list their friends, and navigate the network. However, despite attracting millions of users, SixDegrees.com ceased operation in 2000 after failing to yield a sustainable profit (boyd and Ellison 2007). In 2001, Adrian Scott launched Ryze.com – a social network site devoted to helping people meet business and professional contacts (Ryze.com 2007). While initially intended as a tool for professionals in the high-tech industry to network and organize social events, the service has since expanded to support all types of professional networking activities.

In 2002, Jonathan Abrams, a former Ryze.com user, introduced Friendster.com to compete with online dating sites such as Match.com. Unlike traditional online dating services, Friendster was focused on introducing users to friends-of-friends, rather than strangers, through a social network format. Upon joining the service, users were required to provide demographic information, describe their interests and state their relationship status, as well as a photo and self-description (boyd and Heer 2006). In addition, the service provided a space for users to write 'testimonials' about their friends. As the service grew in popularity, it experienced a series of difficulties. First, its servers and databases were unable to support the explosive growth in users, resulting in frequent service disruptions (danah boyd, Apophenia Blog, entry posted March 21, 2006). Second, social contexts began to collapse[2] as users' employers and former classmates joined the service, creating "an awkward situation as participants had to determine how to manage conflicting social contexts" (boyd 2006b, under "Friending as Context Creating"). Finally, users began using the service for purposes other than those intended by its creator, such as creating 'fake' profiles. In response to the "Fakester"[3] phenomenon, and more specifically profiles that failed to comply with Friendster's standards, Abrams began systematically deleting all profiles that did not adhere to the service's regulations. This practice, termed the "Fakester Genocide," effectively outraged users who argued that the site lost much of its initial appeal once the Fakesters were removed (boyd 2004).

[2] For an explanation on the importance of segregating different social contexts, see section 2.1.1, p. 9

[3] The term "Fakester" was coined to describe the individuals who created fake profiles on Friendster.

While Friendster did not condone fake profiles, MySpace.com – created in 2003 by Tom Anderson to compete with other SNSs – embraced the practice (boyd and Ellison 2007). In fact, MySpace's initial success was due in large part to its acceptance of those individuals that Friendster had rejected or alienated. One group of early adopters, in particular, were indie-rock bands from the Los Angeles area who began creating profiles on MySpace after being kicked off Friendster for failing to comply with profile regulations (boyd and Ellison 2007). Their usage of the space, as a means of self-promotion, subsequently influenced many of their fans to leave Friendster in favor of MySpace. According to boyd and Ellison (2007), "The bands-and-fans dynamic was mutually beneficial: Bands wanted to be able to contact fans, while fans desired attention from their favorite bands and used Friend connections to signal identity and affiliation" (under, "SNSs Hit the Mainstream"). Moreover, this relationship did much to stimulate the initial growth and popularity of MySpace.

By 2004, teenagers began flocking to MySpace. Unlike Friendster, whose user policy banned individuals under the age of 16 from creating a profile, MySpace altered its terms of service agreement to allow minors. The acceptance of underage users, however, became problematic in 2005 when MySpace, after being acquired by News Corporation for $580 million, was caught up in a controversy involving a series of sexual interactions between minor and adult users (boyd and Ellison 2007). Despite this controversy, MySpace continued to dominate the SNS market with a reported 114 million visitors globally between June 2006 and June 2007 (comScore 2007). The media attention garnered from the scandal quite possibly contributed to the substantial growth in users between 2005-2006, particularly among adolescents (boyd and Ellison 2007).

In 2004, Harvard University student Mark Zuckerberg created Facebook.com as a Harvard-only social network site. To join the service, students required a harvard.edu email account. The harvard.edu requirement, according to boyd and Ellison, "kept the site relatively closed and contributed to users' perceptions of the site as an intimate, private community" (2007, under "Expanding Niche Communities"). As the site grew in popularity among the Harvard student population, Zuckerberg began expanding service to all American Ivy League universities, and eventually, all universities and colleges. Each university and college was represented by its own 'network,' and, by default, only people within the same network (university or college) could access each others' extended profiles (Tufekci 2008). In Fall 2005 and April 2006, Facebook began supporting high school students and corporations, respectively. Then, in September 2006, it opened the site to everyone. It should be noted, however, that open access did not mean that users could view extended profiles across the entire site; they continued to require the appropriate 'top level domain' (i.e., .edu) to gain access to closed networks (boyd and Ellison 2007). By April 2007, Facebook had a reported 21 million registered users who were generating approximately 1.5 page views per day (Needham and Company 2007).

While differences exist among the various contemporary SNSs, a core of features can be identified. First, within the site users construct a profile that provides personal information, with the intention of finding or being found by others to create a personal network. Second, most sites allow anyone to join, while requiring user authorization before friendship connections can be made. Finally, upon joining the service, new members are usually asked to provide personal information, such as name, age and email address, as well as a picture of themselves and a self-description. Although there are several different SNSs, some of the most popular include MySpace, Facebook, Bebo and BlackPlanet.com (Hitwise 2008). It should also be mentioned that some SNSs are more popular than others in certain countries and regions, as well as by certain groups of people. For instance, while Facebook is used by approximately 68 percent of the North American user population, only 2 percent of Latin Americans use Facebook (comScore 2007). Table 2-1 (p. 21) provides a breakdown of the market share of U.S. Internet visits to the top ten SNSs from December 2006 to December 2007; Table 2-2 (p. 21) summarizes the worldwide growth of selected SNSs from June 2006 to June 2007. These tables assist in illustrating the extent to which SNSs are used and how much they have grown, in terms of unique visitors, over the course of a one-year period. Table 2-1 indicates that MySpace continues to dominate the U.S. market share with 72.8 percent of users employing this site, and Table 2-2 shows that worldwide SNS usage has grown significantly for selected SNSs from June 2006 to June 2007.

Table 2-1 Market share of U.S. Internet visits to top 10 social network sites

Rank	Name	Domain	Dec-07	Dec-06	% Change
1	MySpace	www.myspace.com	72.32%	78.89%	-8%
2	Facebook	www.facebook.com	16.03%	10.59%	51%
3	Bebo	www.bebo.com	1.09%	0.99%	10%
4	BlackPlanet.com	www.blackplanet.com	1.04%	0.96%	8%
5	Club Penguin	www.clubpenguin.com	0.80%	0.54%	48%
6	Gaiaonline.com	www.gaiaonline.com	0.76%	0.58%	31%
7	myYearbook	www.myyearbook.com	0.73%	0.14%	407%
8	hi5	www.hi5.com	0.63%	0.64%	-1%
9	Classmates	www.classmates.com	0.55%	0.58%	-7%
10	Yahoo! 360	360.yahoo.com	0.54%	0.91%	-40%

Source: Hitwise.com (2008)

Table 2-2 Worldwide growth of selected social network sites

Social Network Site	Total Unique Visitors Jun-06	 Jun-07	 % Change
MySpace	66,401	114,147	7
Facebook	14,083	52,167	270
Hi5	18,098	28,174	56
Friendster	14,917	24,675	65
Orkut	13,588	24,120	78
Bebo	6,694	18,200	172
Tagged	1,506	13,167	774

Source: comScore (2007)

2.2.2. Privacy in Social Network Sites

The widespread adoption of SNSs has led many scholars and the media to examine and raise pragmatic concerns about the disclosure of personal information associated with participation in these sites (Acquisti and Gross 2006; Barnes 2006; Buckman 2005; *CBS Evening News* 2006; Govani and Pashley 2006; Gross and Acquisti 2005; Klein 2006; Lenhart and Madden 2007; Michaels 2006). By their very nature, SNSs encourage users to disclose substantial amounts of personal information such as full name, birth date, sexual orientation, etc. The popularity of these sites, according to boyd and Jenkins (2006), lies in the users' ability to converse with friends, develop an image of themselves, share digital cultural artifacts and ideas, and publicly articulate their social networks. However, despite the benefits listed above, the disclosure of personal information on these sites has led many individuals to question whether or not the gratifications derived from participation in SNSs outweigh the potential privacy risks.

The aim of this section is to review a number of studies and media reports that are relevant to the examination of privacy in SNSs in order to outline key themes in the area.

The focus is in particular on the consequences of revealing personal information in SNSs. While it is not the intention of this thesis to examine the privacy issues that might arise from participation in SNSs, an examination of these issues is important to provide context for investigating the factors that influence information revelation on Facebook.

A primary concern addressed in the privacy and SNS literature is the concept of 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. Barnes (2006) suggests that by freely giving up personal information to join SNSs, individuals open themselves up to a wide range of potential dangers, such as surveillance, sexual predators and identity theft. She contends, "Social networking sites create a central repository of personal information. These archives are persistent and cumulative. Instead of replacing old information with new materials, online journals are archive-oriented compilations of entries that can be searched" (2006, under "A Privacy Paradox"), thus enabling government agencies, school administrators, marketers, and sexual predators, among others, to access and collect data about an individual through their SNS postings. Similarly, Wall Street Journal reporter Rebecca Buckman (2005) calls attention to some of the potential negative social consequences associated with university students revealing very detailed, personal information in Facebook. She reports that some students and university officials have started to worry that in broadcasting their whereabouts at all times and posting personally-identifiable information, such as cell phone numbers and physical addresses, students are placing themselves at a greater risk for stalking and harassment (2005, B1).

Additionally, much of the debate that has surfaced in the media about the disclosure of personal information in SNSs has focused on how these disclosures might negatively affect users' employability. CBS Evening News reporter Sharyn Alfonsi, for instance, reports that "an increasing number of potential employers are accessing these profiles – and using them to decide whom they hire" (*CBS Evening News* 2006). Tom DeMello, owner of the Internet-based company Ziggs, contends that approximately 20 percent of employers are secretly accessing applicants' profiles prior to conducting interviews, and using the information and photographs contained on their sites to assess their character and suitability for employment (*CBS Evening News* 2006). Similarly, Liz

Michaels, director of Career and Planning Services at the University of Chicago, cautions against the disclosure of potentially damaging information in SNSs:

> While employers have long been able to complete a Google search of someone's name, the content on these [SNSs] tend to be much more damaging. Students should assume that whatever is on the Web will be there for a very long time and will come up when anyone, including a future employer, searches for them" (qtd. in *CBS Evening News* 2006).

In Michaels' view, the resources and information made available in SNSs – while potentially useful for employers to build an image of the candidate beyond their résumé – may be detrimental to the applicant's success in finding future employment. In other words, the disclosure of potentially damaging information, such as risqué photos, and evidence of involvement in illegal activities, such as drug use or underage drinking, may influence employers to look elsewhere for a candidate that fits their company's values.

Moreover, media sources also report that several universities and colleges have begun monitoring SNSs in an effort to identify and discipline university code violations (Augustinas 2005; Brown 2008a; Brown 2008b; Jones 2007; Klein 2006; Panja 2007). Northern Star reporter Sarah J. Augustinas (2005), for instance, reported the tale of Ryan Miner, a Duquesne University sophomore, who was punished by university officials for posting a comment on Facebook that the university viewed as homophobic. Similarly, universities such as Oxford and Northern Kentucky have taken disciplinary action against students after discovering photographs posted to SNSs that depicted them participating in illegal activities or behaving in a manner contradictory to university rules. Oxford University even went as far as to fine students $80 to $200 for their involvement in post-exam partying, which consisted of students dousing each other in flour and champagne (Jones 2007; Panja 2007). More recently, Chris Avenir, a first year computer engineering student at Ryerson University in Toronto, was charged with 147 academic offenses, and faced expulsion, for running an online chemistry study group via Facebook designed to assist students with homework assignments (Brown 2008a; Brown 2008b). While Avenir and his supporters argued that "Facebook groups are simply the new study hall for the wired generation" (Brown 2008a), Ryerson University officials contended that sharing tips over Facebook equated to cheating under its academic misconduct policy. In a ruling by the engineering faculty appeals committee, Avenir was ultimately acquitted of all charges and had his passing grade in the chemistry course restored (Brown 2008b). However, the experience has changed Avenir's perspective and has made him much more attentive of Ryerson's policies regarding cheating. Overall, media reports appear to suggest that while SNSs, particularly Facebook, are a great way for students to keep up-to-date on gossip and social events, as well as to assist each other with homework assignments, they are also a valuable and convenient resource for university officials to locate and discipline university code violators.

Finally, apart from surveillance by unwanted audiences, that is, individuals not directly linked to the SNS user, it has also been suggested that the public articulation of one's social network in SNSs is problematic for privacy regulation. Donath and boyd (2004), for instance, report the tale of a 26-year-old San Francisco school-teacher who was faced with a dilemma when her students began joining Friendster. She had joined the network to connect with friends, many of whom had 'crazy' profiles with "suggestive testimonials, risqué photographs, and references to wild times at the Burning Man festival[4]" (2004, 78). While she had changed her profile visibility to 'friends only,' one of her students asked to be a 'friend'. "Although she could edit her own profile to be quite sedate, her friends' profiles were not. Accepting her student's friendship request would [ultimately] reveal her full network to her class" (Donath and boyd 2004, 78). As Goffman (1959) and Coser (1975) contend, individuals try to segment their audiences and their activities in order to occupy different positions so that the individuals who witness them in one of their roles will not be the same individuals who witness them in another of their roles. For example, Coser (1975) states that individuals typically "behave differently at home than at work and relate differently to associates than to family members" (237). However, unlike face-to-face interactions where the individual is often able to fill different roles in different contexts/settings before different audiences in order to "reflect the moral values of the community" (Goffman 1959, 35), in SNSs the public display of one's connections means that the various facets of one's identity (i.e., school-teacher versus Burning Man attendee) may be revealed to one's entire social network. According to Donath and boyd (2004), this creates discomfort not only for the performer

[4] Burning Man is an arts festival that takes place in the Nevada desert during the week leading up to Labor Day. For more information, see http://burningman.com/

who is caught in two contradictory roles, but also for the observer who witnesses the performer in a role incompatible with their perceptions of the performer. Thus, the convergence of different contexts and audiences in SNSs means that the user must be prepared to explain and account for the various roles that they assume as well as their connections to diverse sets of social circles.

The need for Web-based applications that support the segregation of different contexts and audiences has been discussed in detail in Tran et al. (2004) with regard to instant messaging (IM). In their article, the researchers propose the need for IM applications that support multiple concurrent identities (MCIs), which would enable users to present themselves differently to different people simultaneously. In this way, users would be able to designate the types of information and images (or avatars) certain groups of individuals are able to view; thus, minimizing the risks associated with the convergence of contexts and audiences discussed above. Furthermore, in terms of SNSs, the implementation of a set of features that support MCIs, such as the ability to use different profile images for different individuals concurrently, may resolve some of the issues associated with the convergence of contexts and audiences that typically occurs in SNSs.

2.2.3. Reasons for Information Revelation on Social Network Sites

While privacy may be at risk in SNSs, individuals willingly disclose personal information on these sites. In a study of 704 university students, for instance, Tufekci (2008) found that 94.9 percent of Facebook users reported using their full name in their profiles, and two thirds of Facebook and MySpace users had disclosed their sexual orientation and relationship status. Similarly, Gross and Acquisti (2005) found that 82 percent of active Facebook users had disclosed personal information such as their birth date, cell phone number, personal address, political and sexual orientation, and partner's name.

This raises the question: Given the alleged privacy risks and negative social consequences attributed to the disclosure of personal information on SNSs, what influences information revelation on these sites? In their examination of the effects of the Internet on social life, Bargh and McKenna (2004) draw attention to a number of studies and literatures that offer evidence in favor of Internet usage for the psychological well-being of the individual, and the formation and maintenance of close relationships. They suggest that "the main reason that people use the Internet is to communicate with other people over e-mail – and the principal reason why people send e-mail messages to others is to maintain interpersonal relationships" (2004, 575). They state that although early research found that Internet use frequently resulted in negative outcomes, such as increased loneliness and depression (see Kraut et al 1998; Nie and Erbring 2000), subsequent research concluded that greater Internet use was in fact associated with positive social and psychological outcomes (see Kraut et al 2002). For example, Quan-Haase et al. (2002) found that frequent Internet usage adds to (rather than detracted from) participation in organizations and politics, contributes to positive attitudes towards online community involvement, and increases contact with friends and family. In this way, Quan-Haase et al. (2002) suggest that Internet usage provides a variety of social and psychological benefits: 1) it supports social contact by supplementing face-to-face and telephone contact, 2) it enables politically and socially involved individuals to increase their civic engagement, and 3) it provides another means for individuals to connect to and maintain contact with friends and family. This research has shown that Internet use is more likely to extend social contact and online community involvement, rather than produce negative social and psychological outcomes.

The use of the Internet to maintain and form relationships has been further articulated in Lampe, Ellison and Steinfield (2007) with regards to Facebook. Applying the theories of signaling, common ground, and transaction costs, Lampe, Ellison and Steinfield illustrate how profile elements on Facebook enable users to signal aspects of their identity, which should invariably lead to larger personal networks on the site. Signaling theory refers to the different types of personal information that can be disclosed on profiles to signal aspects of the user's identity. These signals can be manipulated by the sender to indicate the specific facets of their identity that they deem important, or interpreted by receivers to assess the characteristics of the sender. Furthermore, in contexts where deception may be beneficial, signaling theory also attempts to explain how signals are kept reliable. Judith Donath contends that "a signal will be reliable if it is beneficial to produce truthfully, yet prohibitively costly to produce falsely" (forthcoming, under "signals, cues and meaning"; see also Donath and boyd 2004; Lampe, Ellison and

Steinfield 2007). In this way, signaling theory provides evidence as to why SNS users should be more apt to reveal accurate personal information on their profiles or information that is playful and comedic rather than intentionally deceptive. Donath and boyd (2004) contend that the public articulation of one's personal network in SNSs provides both implicit and explicit verification on the reliability of one's identity claims. In other words, "the public display of connections found on networking sites should ensure honest self-presentation because one's connections are linked to one's profile; they have both seen it and, implicitly, sanctioned it" (Donath and boyd 2004, 73-74). Therefore, the structure of SNSs should encourage profiles that are more truthful and honest in nature.

Common ground theory and transaction cost theory provide a basis for understanding how the inclusion of large quantities of personal information on SNSs, and in particular accurate personal information, should invariably lead to larger personal networks (Lampe, Ellison, and Steinfield 2007). In terms of common ground theory, Lampe, Ellison and Steinfield contend that the inclusion of profile elements such as location information (i.e., hometown, school name, current city, etc.) and interests should "establish common ground, and … reveal personality aspects that can help people make decisions about declaring friendship links" (2007, 437). Furthermore, they suggest that the ability to search SNS profiles – with or without a potential partner's name – reduces the amount of time spent locating former high school friends, current classmates, or people located in the same university or college dormitory, and therefore reduces the costs of making friendship connections on these sites. Hence, from a simplified transaction cost theory perspective, it should be expected that the more profile elements included in a user's profile, the easier and more accurate a search will be, and the more likely that friendship connections will be established (Lampe, Ellison, and Steinfield 2007). In accord with these theories, Lampe, Ellison and Steinfield (2007) found that there was a positive correlation between populating profile fields on Facebook and the number of friends listed on a user's profile, as well as a weak but positive correlation between the amount of self-descriptive content (i.e., about me, interests, and favorites) revealed and the user's personal network size. These results suggest that high levels of information revelation on SNSs may contribute to increased social interaction and participation, as well as facilitate the maintenance and formation of relationships, as users who disclose more information on these sites also tend to be the individuals with larger social networks; thus, enabling these individuals to interact with a larger group of individuals.

In addition, it has been suggested that the benefits of disclosing personal information on SNSs may negate the potential privacy risks that these disclosures may produce (Donath and boyd 2004; Gross and Acquisti 2005; Lampe, Ellison, and Steinfield 2007). Jenny Sundén (2003), for instance, argues that individuals must first write themselves into being before they can exist online. She states, "to mention that everything [online] must be constructed to exist might appear to be a superfluous statement, but it is useful to point out that no matter how 'ordinary' and 'everyday-like' a character might look, it is the product of a certain (more or less conscious) selection and creation" (Sundén 2003, 77). In terms of SNSs, the information indicated on the user's profile, "signals qualities that relate to the perception of their identity" (Laraqui 2007, 15) and enables them to exist online. For instance, popularity, according to Laraqui (2007), may be signaled by the number of 'friends' in a user's network, the number of groups a user belongs to, the number of comments or testimonials posted to a user's wall, or the number of photographs and/or videos depicting the user engaged in social activities. Laraqui's understanding of SNSs as vehicles for identity performance and construction is further articulated in boyd (in press). In boyd's estimation, social network site profiles enable users to signal meaningful clues about themselves through profile images, self-descriptions, and photo albums, and to receive feedback from their peers and friends, which, in turn, helps with identity formation. She states, "Through profiles, teens can express salient aspects of their identity for others to see and interpret. They construct these profiles for their friends and peers to view" (boyd in press, 13). In this way, the benefits derived from information revelation on SNSs, such as peer acceptance, perceived popularity, and increased social interaction, may influence some users to disclose vast amounts of personal information despite the alleged privacy risks and negative social consequences associated with the disclosure of personally-identifiable information.

Aside from the psychological benefits of disclosing personal information on SNSs discussed above, it has also been suggested that "the fallacy of assuming that only the guilty have to fear the development of intrusive technology (or if you've done nothing wrong you have nothing to hide)" (Marx 1999, Table 1), may contribute to information revelation on the Internet. Marx's contention resonates with the views and opinions of several Internet users. For instance, Viseu, Clement, and Aspinall (2004) report the case of Nicholas who argues that Internet privacy is not a concern because he has nothing to hide and has not experienced any negative consequences. He states:

> I'm not worried about [privacy] and I'm not doing anything about it, and no issues have come up about it either. You don't worry about being broken into until someone breaks into your house ... or some people do things. So, I think if I ever did get hacked I would start worrying about it, but at this point I don't have anything to hide, and don't know why anyone would want to hack the system anyway (103).

In Nicholas' opinion, privacy is not a concern until it has been lost or breached. This viewpoint, according to Viseu, Clement, and Aspinall, may be the product of "years of constant media exposure, in combination with minimal experience of personal privacy problems, [resulting in] people ... reaching a saturation stage and becoming inured to the issue" (2004, 108). In other words, one's own personal experience with Internet privacy, in addition to feelings of resignation and annoyance with privacy concerns, may contribute to and influence the disclosure of personal information online. In terms of information revelation in SNSs, certain users may be more inclined than others to provide vast amounts of personal information in their profiles because they have not experienced any negative consequences as a result of their disclosures in the past, and they do not believe that unwanted audiences would be interested in viewing their profile anyway.

2.2.4. Privacy Protection and Regulation in Social Network Sites

The privacy risks attributed to SNSs have also contributed to an interest in and examination of the strategies users have developed to protect themselves. The Foucaultian theory of the panopticon, for instance, may offer some insight into the use of self-censorship and/or regulation as a mean of addressing these privacy concerns. In *Discipline and Punish* (1979), Foucault suggests that individuals' awareness of constant surveillance influences them to standardize their behavior in order to fall in line with the status quo. He contends that the primary effect of the panopticon is "to induce in the inmate a state of consciousness and permanent visibility that assures the automatic functioning of power" (Foucault 1979, 201). Within the current SNS and privacy literature, several studies have examined whether or not users employ tactics, such as self-censorship, to protect themselves against privacy threats (boyd in press; Govani and Pashley 2006; Gross and Acquisti 2005; Jones and Soltren 2005; Strater and Richter 2007; Tufekci 2008). boyd (in press), for instance, suggests that teenagers "often fabricate key identifying information like name, age, and location to protect themselves" (15). Similarly, in a study investigating audience and disclosure regulation in Facebook and MySpace, Tufekci (2008) found that Facebook users typically optimize their privacy and restrict access to their profiles by unwanted audiences by altering the visibility of the profile to 'only friends' (57.8 percent of Facebook users have changed their profile visibility compared to 41 percent of MySpace users) and MySpace users frequently use nicknames or monikers instead of their real names in their profiles (62.7 percent of MySpace users use their real name compared to 94.9 percent of Facebook users).

A few studies have shown that despite expressing an awareness and concern about Internet privacy, users seldom provide false or inaccurate information, and very rarely change their default privacy settings (Acquisti and Gross 2006; Govani and Pashley 2006; Gross and Acquisti 2005). For example, Govani and Pashley (2006) found that less than 25 percent of students had altered the visibility of their profile on Facebook, thereby allowing unknown individuals to access their profile. It is unclear why these differences in findings exist in the current literature on privacy in SNSs. Given that the two studies discussed above (Tufekci 2008 and Govani and Pashley 2006) were conducted two years apart, a possible explanation is that over time students may have become more aware of the privacy implications associated with SNSs and may have started to manage their privacy concerns by enacting protective measures. It is the intention of this thesis therefore to ask student directly in interviews about their privacy protection strategies in order to expand the research in this area.

The literature on privacy, both offline and online, and SNSs was summarized. While the literature is extensive in each of these areas, the review focused on studies, reports and theories that were pertinent to the present study. The next chapter outlines the research questions and hypotheses used to guide the study, and the methods employed for data collection.

CHAPTER 3
RESEARCH METHODS

3.1. INTRODUCTION

This chapter serves four purposes. First, it outlines the research questions and hypotheses used to guide the study. Second, it provides an overview of the research design employed to examine the research questions and hypotheses. Third, the chapter describes the sample, recruitment process and research procedures. Finally, the chapter concludes with a description of how variables were measured and the data were analyzed.

3.2. RESEARCH QUESTIONS AND HYPOTHESES

Two research questions guided the study. The first research question investigated the factors influencing information revelation on Facebook. The second research question examined the factors that influence privacy protection and the strategies undergraduate students have developed to protect themselves against privacy threats while using Facebook. Chapter 1 provided a comprehensive description of the research questions examined in this study (see section 1.3, p. 5). Based on the literature review discussed in Chapter 2 and the research questions outlined above, five hypotheses were formulated.

3.2.1. Information Revelation on Facebook

Research has demonstrated that concern for Internet privacy has an effect on the information revelation habits of Internet users (Pew 2000; Tufekci 2008; Viseu, Clement and Aspinall 2003). In her examination of trust and privacy online, Susannah Fox for the Pew Internet and American Life Project found that out of 45 percent of individuals who have not provided real personal information to access a Web site, 61 percent identify themselves as 'hard-core privacy defenders' and refuse to provide personal information in order to use an Internet site. She writes that: "This hard-core group is more likely to believe that [Internet] tracking is harmful, that online activities are not private, and that there is reason to be concerned about businesses getting their personal information" (Pew 2000, 9). By contrast, as discussed in the literature review, individuals with a comparably low level of concern for Internet privacy, such as those who hold the belief that privacy is only a concern when it has been lost or breached, tend to be more willing to disclose personal information online. For example, Viseu, Clement and Aspinall (2003) found that individuals who held the belief that privacy is only a concern when it has been lost or breached tended to perceive the benefits of disclosing personal information in order to use a site to be greater than the potential privacy risks associated with disclosure (103). In other words, Internet privacy is not a concern for these individuals because they have not experienced any negative consequences as a result of their disclosure of personal information in the past. Therefore, it is expected that:

H1 Concern for Internet privacy will be negatively associated with information revelation on Facebook.

According to Susannah Fox for the Pew Internet and American Life Project (2000), large percentages of Internet users are concerned about unwanted audiences obtaining information about them or their families (86 percent), hackers accessing their credit card information (70 percent), or someone finding out personal information from their online activities (60 percent). Similarly, Acquisti and Gross (2006), in their study examining information sharing and privacy in Facebook, found that students showed high levels of concern for general privacy issues, such as a stranger finding out where they live and the location and schedule of their classes (*M*=5.78 on a 7-point Likert scale), and a stranger learning their sexual orientation, name of their current partner, and their political affiliations (*M*=5.55). This research shows that Internet users are concerned about unwanted obtaining private and personal information about them.

Despite these concerns, research has shown that users continue to disclose personal information and often disclose accurate personal information (Acquisti and Gross 2006; Govani and Pashely 2006; Gross and Acquisti 2005; Pew 2000; Tufekci 2008; Viseu, Clement, and Aspinall 2003). Acquisti and Gross (2006), for instance, found that 89 percent of Facebook users at Carnegie Mellon University reported using their full name in their profiles, 87.8 percent had revealed their birth date, and 50.8 percent had listed their current address. There is some evidence, however, that suggests that the more concerned an individual is about online breaches of privacy, the less likely he or she is to disclose certain personal information. For example, Tufekci (2008) revealed that concern about unwanted audiences had an impact on whether or not students disclosed their real name in MySpace, and whether or not students disclosed their religious affiliation on MySpace and Facebook. These findings suggest that there may be an association between an individual's concern about unwanted audiences accessing their profile and the amount and types of information they reveal on Facebook. Therefore, it is predicated that:

H2: Concern about unwanted audiences will be negatively 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, this process of writing oneself into existence occurs with the construction of a profile that reveals personal information about the user. Through the inclusion of profile elements, such as a self-description, a statement of one's relationship status, a description of one's interests, and a self-image, users are able to signal aspects of their identity to their peers and friends (boyd in press; Laraqui 2007). According to Gross and Acquisti (2005), one of the strongest motivating factors influencing users to provide more information than is required for participation in SNSs is to reveal enough information to make the site useful and beneficial for both the user and other people using the service. Furthermore, Jones and Soltren (2005) found that users with large social networks tended to be much more forthcoming with their personal information. For instance, they found that large percentages of users with more than 300 friends disclosed more information concerning their interests (85.3 percent compared to 64.1 percent), favorite music (82.9 percent compared to 64 percent), and clubs (81 percent compared to 51.5 percent) than users with smaller networks. Therefore, it is predicted that:

H3: Network size will be positively associated with information revelation on Facebook.

3.2.2. Privacy Protection in Facebook

One way of examining privacy protection in Facebook is by examining the concept of profile visibility. Profile visibility can refer to outside visibility – that is, to whom the users' profile is currently visible – and inside profile visibility – that is, to whom the users' information within Facebook is visible. In terms of outside visibility, for example, SNSs typically allow users to alter the visibility of their profile in order to restrict unwanted audiences from accessing their profile and viewing the information contained within. On Facebook, users can set their outside profile visibility to one of four levels: 'all networks and all friends', 'some networks and all friends', 'friends-of-friends', and 'only friends'. In her examination of audience and disclosure regulation on MySpace and Facebook, Tufecki (2008) found that there was an association between students' concern over their profile being found by unwanted audiences and their level of profile visibility; for each level of increase in their concern about unwanted audiences, students were 40 percent less likely to set their profile visibility to all networks and all friends. These findings suggest that it is likely that an individual's concern about unwanted audiences will affect their level of outside profile visibility. Therefore, it is expected that:

H4 Concern about unwanted audiences will be negatively associated with profile visibility on Facebook

In addition to concern about unwanted audiences accessing the user's profile, it seems likely that an individual's concern for Internet privacy will also affect their level of profile visibility on Facebook. Therefore, it is also expected that:

H5 Concern for Internet privacy will be negatively associated with profile visibility on Facebook

This section described the five hypotheses derived from the literature review. The hypotheses are summarized in Table 3-1

Table 3-1 Summary of hypotheses

H1:	Concern for Internet privacy will be negatively associated with information revelation in Facebook
H2:	Concern about unwanted audiences will be negatively associated with information revelation in Facebook
H3:	Network size will be positively associated with information revelation on Facebook
H4:	Concern about unwanted audiences will be negatively associated with profile visibility in Facebook
H5:	Concern for Internet privacy will be negatively associated with profile visibility on Facebook

3.3. RESEARCH DESIGN

3.3.1. Mixed Methods Approach

To address the research questions and hypotheses outlined above, a mixed methods approach to research was considered ideal for three reasons. First, using a mixed methods approach allows for the combination of multiple data collection methods and sources of information, enabling a more comprehensive understanding of the research questions than would be possible with either quantitative methods or qualitative methods alone (Creswell and Clark 2007). In the present study, a combination of questionnaires, semi-structured interviews, and Facebook profile analyses were used to address the research problem. Second, mixed methods research affords the researcher opportunities to harness the strengths of some methods to offset the weaknesses of others (Axinn and Pearce 2006). In view of the fact that "all methods have [their own] strengths and weaknesses, combinations of multiple methods that achieve this counterbalancing aim are particularly valuable" (Axinn and Pearce 2006, 2). The present study, for instance, used the strengths of qualitative methods in eliciting the views and opinions of participants to counterbalance some of the weaknesses of quantitative methods. Third, employing a mixed methods approach allows for the elaboration and expansion of the results from one method with the results from another method (Creswell 2003). In the present study, the qualitative findings were used to expand and explain the quantitative results.

3.3.2. Surveys

Survey research has been widely used in the social sciences as a method for collecting observational data (Babbie and Benaquisto 2002). Typically, survey research involves the researcher selecting a sample of respondents and administering a set of standardized questions. The data generated in surveys can then be used for descriptive, explanatory and exploratory purposes. In the present study, survey data were used to describe and explain the information revelation practices and privacy protection strategies of a sample of undergraduate students at the University of Western Ontario (see section 3.5.1, p. 41 for a description of the sample population).

There were two main reasons for using survey research to measure information revelation and privacy protection on Facebook. First, surveys are particularly beneficial to the present study because previous research has demonstrated the effectiveness of questionnaires in obtaining data on information revelation and privacy protection in SNSs. For example, Tufekci (2008) found in a large-scale survey of university students that information revelation was highly influenced by factors such as gender, future audiences and general privacy concerns. This study continues this line of research.

Second, survey research was the best method for obtaining an ample amount of original data in a relatively time-efficient and cost-effective manner. Given the time constraints imposed on Master's thesis research, a method was needed that allowed me to collect data on undergraduate students in a relatively short time span. Surveys enable me to collect significant amounts of numeric data that could be used to measure overt behaviors and descriptive aspects of a "population by studying a sample of that population" (Creswell 2003, 153), thus reducing the amount of effort spent on data collection. Furthermore, the standardization of questions typically associated with survey research provides data in the same form from all respondents (Babbie and Benaquisto 2002) and therefore can be used for purposes of comparability. The present study used standardized questions as much as possible.

As with any research method, however, surveys have their limitations. One major disadvantage of survey research is that participants cannot express their opinions in detail, making it difficult to pursue issues and topics in greater depth. Therefore, in order to address the deficiencies of survey research, qualitative interviews and profile analyses were also conducted. A discussion of these methods will now be provided.

3.3.3. Semi-Structured Interviews

There were two key advantages to using semi-structured interviews to further investigate information revelation and privacy protection on Facebook. First, a semi-structured interview technique enables the researcher to gain a first-hand account of respondents' attitudes and opinions through focused, conversational, two-way communication (Babbie and Benaquisto 2002; Creswell 2003). A primary focus of the study was to examine the factors that influence information revelation and privacy protection on Facebook, as well as the strategies that undergraduate students have developed to protect themselves against privacy threats. To study these variables, a method was needed that is capable of collecting detailed information on undergraduate students' perceptions and attitudes towards the disclosure of information on Facebook and their employment of privacy protection strategies. Semi-structured interviews, as indicated above, enable the collection of these types of data through in-depth conversations with participants

Second, semi-structured interviews are often more flexible than structured methods such as surveys. This flexibility provides the respondent with more freedom to "change the course of the conversation and bring up new issues that the researcher had not preconceived" (Axinn and Pearce 2006, 6). It also enables the researcher to probe and follow-up with additional relevant questions when new issues arise that do not directly follow from the prepared line of questioning (Babbie and Benaquisto 2002). In this way, semi-structured interviews often uncover new insights and topics that the researcher had not considered prior to the interview, providing more depth to the study.

3.3.4. Profile Analyses

Profile analyses were conducted in conjunction with the semi-structured interviews and were used to provide visual confirmation of respondents' use of Facebook. These profile analyses consisted of viewing the interview subjects' profile, with their consent, and examining the information disclosed on their main profile page, the privacy settings they have activated, and the actual number of friends in their personal network. The intent of the profile analyses component was to both confirm the information provided by the respondent during the interview, providing a second source of information, and also to probe the respondent further about their information revelation practices and privacy protection strategies.

In sum, the research design consisted of employing a mixed methods approach whereby data were collected through questionnaires, semi-structured interviews and profile analyses. The methods employed in this study were used to provide a more comprehensive understanding of the research problem than would have been possible with just one method alone. The data gained from the methods were used to examine the information revelation practices, habits and behaviors of undergraduate student Facebook users and the various ways they protect themselves against privacy threats. A potential concern of the study and its use of multiple data collection techniques is that the data from the different sources will contradict each other. In the event that this occurs, I will take into consideration the possible reasons for the contradiction and provide justification explaining the contradicting data. The process used to collect the data will now be discussed.

3.4. DATA COLLECTION PROCESS

3.4.1. General Overview

The data for the study were collected using questionnaires, interviews and profile analyses. Ethics approval was obtained for the study (see Appendix I, p. 109, Ethics Approval) and all participants were given an information letter outlining the purpose of the study, incentives and confidentiality (see Appendix A, p. 84, Information Letter to Questionnaire Participants; Appendix B, p. 86 Information Letter to Interview Participants).

Participant recruitment was conducted in two sequential phases: phase one and two involved recruiting participants for the questionnaire and interviews and profile analysis, respectively. In the first phase, students enrolled in one of two media, information and technoculture courses at the University of Western Ontario were asked at the beginning of one of their lectures to complete a paper-and-pencil based questionnaire. The questionnaires were distributed to willing participants either at the conclusion of their lecture or during break. Students were then asked to return the completed questionnaires at the conclusion of the lecture, in tutorial, or at their subsequent lecture. Participation was voluntary and the course instructors were not informed about who participated and who did not. All questionnaires returned within one week of the initial distribution were included in the final analysis.

In phase two, participants for the interviews were recruited through advertisements posted to bulletin boards throughout the University of Western Ontario. Interested students were asked to contact the researcher via email or telephone. Twenty-four students responded to the advertisement and agreed to participate in the study. Interviews were scheduled at times convenient for the participants. Three students, however, failed to show-up for their scheduled interview, reducing the sample size to twenty-one: 5 male students (24 percent) and 16 female students (76 percent). While an equal distribution of males and females was initially sought, it proved difficult to secure interviews with male students. First, significantly fewer male students showed interest in participating in the study. Second, nearly half of the male students scheduled for an interview failed to show up for their scheduled appointment. Finally, attempts made to reschedule interviews with male students who missed their initial appointments proved ineffective because they failed to respond to a subsequent email.

3.4.2. Questionnaire

The questionnaire was the primary data collection tool, and all students enrolled in the two media, information and technoculture courses were asked to complete it. The questionnaire was self-administered to students between October and November 2007. To ensure consistency of results, the same paper-and-pencil based questionnaire was administered to both classes. The completed questionnaires were stored in a locked cabinet to protect the data (see Appendix D, p. 89, for the questionnaire).

The questionnaire consisted of four parts. The first part contained questions about respondents' adoption and use of Facebook. The second part contained questions about respondents' level of concern for Internet privacy, their information revelation habits, practices and behaviors both within and outside of Facebook, and the perceived likelihood of unwanted audiences accessing their profiles.

The third part consisted of privacy protection questions, designed to elicit the possible ways respondents protect themselves against privacy threats in Facebook, such as altering their default privacy settings or using self-censorship tactics.

The fourth part requested demographic information on each respondent, including their age and sex, to be used as controls in the final analysis. Details on the questionnaire items are included at the conclusion of this chapter, under section 3.5 Data Analysis and Measures.

As the questionnaire was the primary data collection tool, the following steps were taken to ensure a high completion and return rate (Babbie 2002; de Vaus 1995; Dillman 1978; Dillman et al. 2008; Mitzes, Fleece, and Roos 1984)

(1) To maximize motivation to participate in the study, all potential respondents were offered a chance to win one of four Tim Hortons gift certificates valued at $10 each.

(2) To reduce reluctance to participate, respondents were given an opportunity to ask questions and have any concerns about the study addressed prior to receiving the questionnaire. Respondents were also given an information letter, which provided information about confidentiality, incentives and the purpose of the study (see Appendix A, p. 84, Information Letter).

3.4.3. Semi-Structured Interview Technique

The interviews were semi-structured and included questions about respondents' adoption and use of Facebook, information revelation practices, concern for Internet privacy, and privacy protection strategies (see Appendix E, p. 100: Interview Guide). In addition, the interviews contained a visual component in which respondents were asked to show the researcher their Facebook profile, including their privacy settings, network size, and the information indicated on their main profile page. These profile analyses were used to confirm the information obtained in the interviews and questionnaires. The profile analyses were voluntary and the respondents were informed of their right to refuse participation.

A semi-structured interview technique was chosen because it is based on an interview guide, which provides a framework for the interview and lists all the important topics and points to be discussed by the respondents (Legard, Keegan, and Ward 2003). It also allows for focused, conversational, two-way communication between the researcher and participant, and for the improvisation and/or updating of questions when relevant information or interesting tangents arise from the course of the interview process that do not directly follow from the prepared line of questioning (Babbie 2002; Legard, Keegan, and Ward 2003).

The interviews were scheduled in advance and took place in a mode chosen by the participant: face-to-face in one of the meeting rooms at the University of Western Ontario, via email, instant messaging or over the telephone. While the use of different modes of data collection has potential biases, such as the concern of whether or not respondents who respond by one mode will provide the same answers had they responded by another mode (Dillman et al. 2008), the decision to provide participants with a range of interviewing options was intended to make participation in the study comfortable and convenient for potential respondents, Moreover, it was intended to provide respondents unable to meet in person with an opportunity to participate in the study. Despite the range of interviewing options, however, only two respondents opted for an email-based interview, while the remainder chose a face-to-face interview.

The face-to-face interviews lasted in duration from 15 to 30 minutes, and were conducted privately in a meeting room at the University of Western Ontario to ensure participant confidentiality. Consent was obtained from each informant to audio-tape record the face-to-face interviews to guarantee accuracy and data quality (see Appendix C, p. 89: Consent to be Interviewed). After every interview conducted face-to-face, notes on the researcher's impressions or any additional information that seemed relevant were recorded on the back of the interview guide. The interview guides, consent forms, and email-based transcripts were stored in a locked cabinet to protect the data.

3.5. DESCRIPTION OF SAMPLE

3.5.1. Description of Questionnaire Sample

Eighty-five participants were initially recruited from undergraduate students enrolled in media, information and technoculture courses at the University of Western Ontario. The sample was reduced to seventy-seven after non-users were removed from the sample. Non-users (8.2 percent) were removed because the focus of the study was on the information revelation and privacy protection practices of Facebook users. Despite being invited to take part in the study, approximately 200 students chose not to respond. This yielded a response rate of roughly 28.3 percent. The decision to survey students in media, information and technoculture was for convenience – that is, the population was chosen because of participant availability and the ease in which participant recruitment could be conducted. This sampling method, however, has two potential biases. First, since participation was voluntary, it is possible that certain types of people chose not to respond. This is problematic in that those who refused to participate in the study could have provided different answers and perspectives than those who agreed to participate. Second, it is likely that media, information and technoculture students will be more media savvy than students in other academic disciplines and will have a better understanding of the issues and concerns related to privacy in SNSs. This could be problematic in that expressed concern for privacy in SNSs may be higher than if students from different disciplines had been surveyed. As a result, this particular sample might show unique patterns that are not applicable to the general population of students.

Respondents ranged in age from 17-25 years, with a median age of 19 years. Male respondents were underrepresented in the questionnaire (n=20 or 26 percent) in comparison to female respondents (n=55 or 71.4 percent), and two respondents declined to provide this information. While this could suggest that the sample is biased, information obtained from the University of Western Ontario on the full-time constituent enrollment by faculty and gender for 2006-2007 reports that female students represent 71.4 percent of the media, information and technoculture student population while male students only account for 28.6 percent. Thus, the bias is representative of the media, information and technoculture student population and no weighting for gender was conducted in the analysis.

3.5.2. Description of Interview Sample

The numerical data were supplemented with in-depth interviews and profile analyses from a sample of undergraduate students enrolled in a variety of academic disciplines at the University of Western Ontario. The decision to use students from different disciplines was to enable a broader and more in-depth examination of the range and diversity of perceptions related to information revelation and privacy protection in Facebook, particularly in view of the fact that the questionnaire sample was so narrow. Participants were recruited through advertisements posted to bulletin boards at the University of Western Ontario. This yielded a sample of twenty-one individuals, nineteen of whom volunteered to participate in both the face-to-face interview and profile analyses. The remaining two individuals volunteered to participate in an email-based interview, which did not allow for an examination of their Facebook profiles. Similar to the questionnaire, male respondents were underrepresented in the interviews: there were 5 male students (24 percent) and 16 female students (76 percent). A diverse sample was initially sought but proved difficult because male respondents did not show a comparable degree of interest in the study as their female counterparts. The majority of students were enrolled in social sciences and humanities (47.6 percent), followed by sciences (23.9

percent), business (9.5 percent), and music (9.5 percent), and two students were working towards a combined degree (9.5 percent).

The face-to-face interviews and profile analyses were conducted simultaneously, and lasted between 15 to 30 minutes. To ensure participant confidentiality, each respondent was assigned a pseudonym and all identifying characteristics were omitted from the transcriptions. Table 3-2 summarizes the key characteristics of the interview sample.

Table 3-2 Description of interview sample

Field of Study	*Pseudonym*	*Age*	*Year of Enrollment*
Social Sciences and Humanities (10)	Michael	32	3rd year
	Rachel	26	1st year
	Melanie	20	3rd year
	Leanne	23	5th year
	Cheryl	18	1st year
	Alexandra	20	3rd year
	Rebecca	22	4th year
	Tara	21	4th year
	Melinda	25	4th year
	Brian	18	1st year
Sciences (5)	Justine	20	3rd year
	Diana	25	4th year
	Charlie	23	4th year
	Elizabeth	24	1st year
	Ashley	23	1st year
Business (2)	Lori	21	3rd year
	Christine	18	1st year
Music (2)	Samantha	20	2nd year
	Andrew	20	2nd year
Combined Degrees (2)	James	21	3rd year
	Anna	19	2nd year

3.6. MEASUREMENT AND DATA ANALYSIS

To test the hypotheses outlined in section 3.2, quantitative data collected through a paper-and-pencil based questionnaire were used exclusively. The qualitative data were also analyzed, not to test the hypotheses but to assist in explaining and understanding the quantitative findings. This section commences by outlining the measures used to test the hypotheses. Then, the quantitative and qualitative data analysis procedures, respectively, are discussed.

The instrument included five broad types of measures, which are discussed in more detail below. Demographic information was collected on respondents, including gender and age. Facebook usage and adoption measures were also included, such as time spent using Facebook and reasons for adoption. The instrument also included measures of information revelation, privacy concern, and privacy protection strategies.

3.6.1. Measures

3.6.1.1. Facebook Adoption

To investigate respondents' reasons for adopting Facebook, a measure was adopted from Govani and Pashley (2006): "What was your primary motivation(s) for joining Facebook?" Respondents were instructed to check all reasons that applied to their situation. The items were coded as 0="no" and 1="yes". See Table 4-1 (p. 50) for a list of the items.

3.6.1.2. Facebook Usage

The instrument included three measures of Facebook usage. The first measure was adopted from the Pew Internet and American Life Project's (PEW) "Social Networking Websites and Teens Survey" (2007) and was used to examine respondents' frequency of Facebook visits: "How often do you visit Facebook?" For the first assessment, respondents indicated their frequency of use on a 8-point scale (1="several times a day"; 2="once a day"; 3="several times a week"; 4="once a week"; 5="several times a month"; 6="once a month"; 7="a couple of times a year"; 8="never". They were also given the option to respond: 9="don't know/refused".

A similar measure was employed to examine the length of time a respondent spent using Facebook last week: "On average, how much time did you spend everyday on Facebook last week?" Respondents reported their total hours and minutes using Facebook last week.

The third measure asked respondents to report the year and month that they adopted the service. The number of years and months reported by the respondent was subsequently converted to years to provide a numeric representation that was easier to comprehend. For example, 1 year and 6 months was coded as 1.5 years. These three assessments assist in understanding the extent to which respondents use Facebook and the length of time they have been using the service.

3.6.1.3. Personal Network Size

A measure was created to learn about the average size of respondents' personal networks. This measure consisted of five parts and asked respondents to first report their total number of Facebook friends and then to indicate how many of these total friends they considered to be close friends, acquaintances, distant friends, and people that they had only met on Facebook. The term 'distant friends' was removed from the final analysis because several respondents were unable to distinguish 'distant friends' from 'acquaintances'.

3.6.1.4. Information Indicated on Profile

In order to investigate respondents' information revelation practices, a modified scale adopted from Govani and Pashley (2006) was used. Questions were added to include a larger set of information items than was provided by Govani and Pashley. Respondents were asked to indicate which of several salient profile elements (such as relationship status, e-mail address, and cellular phone number) they included in 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 17 types of information that could be revealed. These items offer insight into the degree to which respondents are willing to reveal personal information on Facebook. See section 4.2.1 (p. 54) for item wording and the frequency distribution of the items.

3.6.1.5. Concern for Internet Privacy

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

3.6.1.6. Concern about Profile Access by Unwanted Audiences

In addition to measuring general concern for Internet privacy, respondents were also asked to indicate, from 7 attitudinal questions, to what extent they agree that unwanted audiences (such as current or future employers, university admissions officers, and sexual predators) have begun accessing Facebook profiles in order to use the information contained within for a variety of potentially harmful purposes. The answers to these questions were reported on a 5-point Likert-scale where 1="strongly disagree"; 2="disagree"; 3="neither disagree nor agree"; 4="agree"; and, 5="strongly agree". Based on the items, an additive scale was created that measured respondents' concern about unwanted audiences accessing their profile. The scale was used to provide insight into the degree to which respondents believe that unwanted audiences might access their profiles. Table 3-3 provides the means and standard deviations for each item.

Table 3-3 Concern about unwanted audiences

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

3.6.1.7. Profile Visibility

The instrument included two measures of profile visibility. The first measure was adopted from the "PEW Social Networking Websites and Teens Survey" (2007) and assessed respondents' level of outside profile visibility – that is, the extent to which their profile is accessible by other Facebook users. Respondents were asked to indicate to whom their profile is currently visible. The outside 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".

The second measure was adopted from Govani and Pashley (2006) and assessed respondents' level of inside profile visibility – that is, the extent to which various aspects of respondents' profiles are visible to other users. Respondents were asked to indicate, from 8 information types, to whom their information is currently visible. The inside profile visibility levels were coded as: 1="visible to only me"; 2= "visible to only my friends"; 3="visible to some of my networks and all of my friends"; 4="visible to all my networks and all my friends". The items were added up in a single scale, ranging from 1-8, and measured whether respondents' information is restricted or visible to others. See section 4.3.1 (p. 58) for the item wording and frequency distribution of the items.

3.6.1.8. Privacy Protection Strategies

In order to further 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 section 4.3.3 (p. 62) for item wording, means and standard deviations.

3.6.1.9. Communication Practices on Facebook

This measure was adopted from the PEW "Social Networking Websites and Teens Survey" (2007) and was used to investigate respondents' use of Facebook's communication tools as a protective measure. Respondents were asked to indicate whether or not they ever (1) post messages to a friend's wall or (2) send private email messages to a friend within Facebook. The measure provides insight into the communication practices of respondents and the extent to which they use these tools to communicate with their friends and peers on Facebook.

3.6.2. Data Analysis

3.6.2.1. Quantitative Data Analysis

The quantitative data were analyzed using descriptive statistics and correlations. Descriptive statistics were used primarily to provide an overview of the distribution of variables with regards to respondents' adoption and use of Facebook, as well as to examine the types of privacy protection strategies employed most often by undergraduate students. Correlations were used to test the hypotheses.

3.6.2.2. Qualitative Data Analysis

All interviews conducted face-to-face (n=19) were audio-taped and transcribed. Notes were taken during the profile analyses phase and the participants' conversations were recorded. The transcripts from the interviews and profile analyses were then analyzed using a framework-based approach, which consists of classifying and organizing the data according to key themes, concepts and categories (Ritchie, Spencer, and O'Connor 2003). The themes were derived from the topics covered in the interview guide (see Appendix E, p. 100: Interview Guide). The main themes were then subdivided into a succession of related subtopics (Ritchie, Spencer and O'Connor 2003). This produced a thematic framework from which the data could be analyzed (see Appendix F, p. 104 Thematic Framework).

Each main theme was displayed in its own matrix on an Excel spreadsheet with the subtopics listed in the columns and the respondents denoted in the rows (see Appendix G, p. 105: Thematic Framework Matrix). Data from each respondent were then synthesized and placed under the appropriate subtopic(s) of the thematic framework. This allowed me to identify the different elements, constructs and categories that emerged within a particular subtopic and to understand the range of data that exist. The data from the interviews and profile analyses were used to enhance the quantitative analysis. The qualitative data provide insight into the uniqueness of the respondents with regard to their information revelation practices and privacy protection strategies.

In sum, the data of the present study consisted of quantitative data collected through a questionnaire and qualitative data collected through interviews and profile analyses. The quantitative data measured the extent to which Facebook is integrated into the social life of respondents, the types of information posted to respondents' profile and the tactics employed by respondents to protect themselves against privacy threats while using the service. The qualitative data obtained from the interviews and profile analyses were transcribed and organized in a thematic framework, providing a detailed picture of respondents' information revelation and privacy protection on Facebook, which was essential for explaining the quantitative results.

In this chapter, the measures employed in the study were discussed and the data analysis procedures for each method were outlined. The following chapter presents the results of the study.

CHAPTER 4
STUDY RESULTS

4.1. FACEBOOK ADOPTION AND USAGE

This section examines undergraduate students' use and adoption of Facebook to provide the necessary context to examine information revelation and privacy protection practices of student users of Facebook. The aim of this section is to better understand the extent to which Facebook is integrated into the social life of the undergraduate student to provide a rationale for selecting the current sample.

4.1.1. Facebook Adoption

To investigate undergraduate students' adoption of Facebook, respondents were asked in the questionnaire to indicate their reasons for joining the service. The data show that 85.5 percent of undergraduate students joined Facebook because a friend suggested it, 48.7 percent because all of their friends were already users, and 46.1 percent because Facebook provided an additional means to keep in touch with friends. By contrast, few students reported joining Facebook to meet new people (6.6 percent), to find dates (2.6 percent) or to network (6.6 percent), suggesting that Facebook adoption occurs predominantly to maintain and support one's already established social network, and that network expansion (or relationship initiation) is not a primary objective (see also Table 4-1: Reasons for adoption).

Table 4-1 Reasons for adoption

Individual Items	Percent
Friend suggested it	85.5
Received a promotional email	6.6
Everyone I know is on Facebook	48.7
Find classmates	18.4
Find course information	2.6
Find people with mutual interests	1.3
Get to know more people	6.6
Help others to keep in touch with me	46.1
Find dates	2.6
Find jobs	0.0
Network in general	6.6

Besides the three factors of Facebook adoption discussed above, the interview data also show that undergraduate students' decision to join Facebook is partly influenced by peer pressure and a desire for social inclusion. In terms of the former, a few participants noted that they were pressured into joining Facebook rather than adopting the service voluntarily. For example, Diana, a 25-year-old science major, reported that she had adopted Facebook as a result of her friends refusing to send photos via email and indicating that they would be posting them exclusively on Facebook. This tactic, according to Diana, was used to ensure her adoption. All her friends were already users and several had expressed a desire for her to join. Thus, by making the photos available only on Facebook, they could guarantee her adoption of the service.

In terms of social inclusion, the interview data show that several respondents joined Facebook to be kept abreast of social events. For example, Ashley, a 23-year-old science student, stated that Facebook was the only place to receive up-to-date information on parties, and that this motivated her to adopt Facebook. Similarly, Melinda, a 4th year humanities student, noted that while she initially joined Facebook out of curiosity, she only logged onto the service to receive invitations to events. The experiences of Melinda, Ashley and others suggest that Facebook adoption is at least partially influenced by a desire to be kept informed of social activities as well as for inclusion and participation with members of one's offline social network.

4.1.2. Facebook Usage

In line with previous research, the questionnaire data showed that undergraduate students are heavy users of Facebook. Indeed, 81.8 percent reported logging into their Facebook account "several times a day" and using Facebook for an average of 3 hours and 48 minutes per week (*M*=3.8; *S.D.*=3.89; see also Figure 4-1). The data also showed that students have been using Facebook for approximately one and a half years (*M*=18.34; *S.D.*=7.37; see also Figure 4-2).

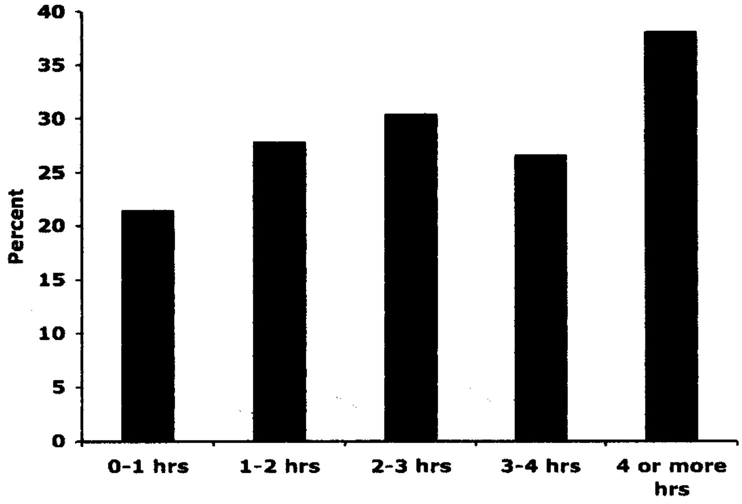


Figure 4-1. Hours using Facebook last week

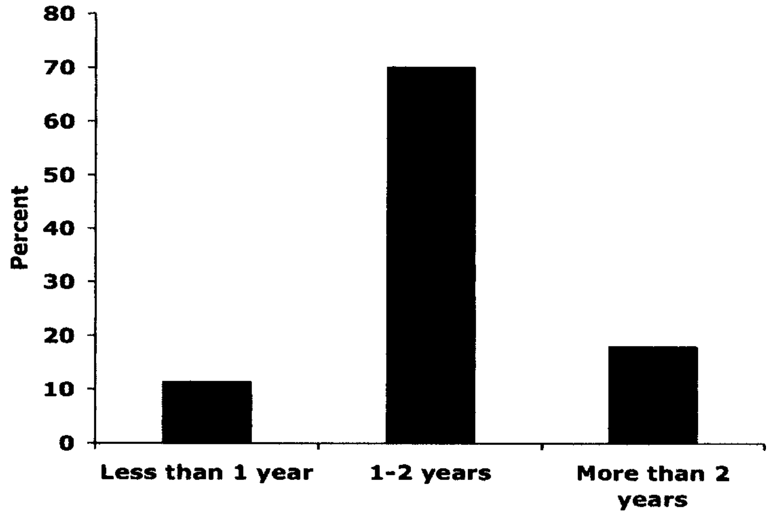


Figure 4-2. Length of time using Facebook

The interview data showed that while respondents use Facebook extensively and log into their accounts between 2 to 5 times per day on average, the length of each log in session varied. On the one hand, respondents reported spending 5 to 15 minutes per session to quickly check and/or receive messages, view photographs, check-up on the activities of their friends or access information on upcoming social events. On the other hand, a few respondents reported spending significantly longer periods of time on

Facebook when they wanted to procrastinate or 'creep'[5] other users. In these instances, respondents reported spending up to an hour navigating the network, reading profiles, and looking at photographs.

4.1.3. Personal Network Size

Facebook users generally sustain an exceptionally large network of friends (Gross and Acquisti 2005). The mean number of friends reported in respondents' personal network was 401.62 (*S.D.*=198.64; see also Table 4-2: Personal network size). Furthermore, the data show that the majority of the friends listed in respondents' networks were acquaintances (*M*=195.45, *S.D.*=127.44) rather than close friends (*M*=67.75, *S.D.*=80.28). These results suggest that the concept of "Friendship" as defined in Facebook extends beyond those individuals that the user shares a strong connection and often includes weak ties[6] (see boyd 2006a; Tufekci 2008).

Table 4-2 Personal network size

	M	*S.D.*
Total friends	401.62	198.64
Close friends	67.75	80.28
Acquaintances	195.45	127.44
Met only on Facebook	5.31	11.37

The interview data further support the quantitative findings, showing that undergraduate students' personal networks are typically comprised of all individuals that he or she would feel comfortable interacting with in an offline context. For example, Andrew, a 2nd year music student, reported that his decision to 'friend' someone is based on whether or not he would feel comfortable walking up to them in person and engaging in conversation. Similarly, for other respondents, the act of 'friending' was influenced by whether or not they would be able to say hello if they met them on the street. Thus, for Andrew and others, friendship on Facebook consisted of all individuals – regardless of whether they were a close friend or an acquaintance – that they would feel comfortable interacting with in an offline setting.

[5] Creeping refers to the act of viewing other people's pages, reading their profiles, and staring at their pictures without ever interacting.

[6] Weak ties, also known as acquaintances, have been defined by Granovetter (1983) as individuals who do not provide the same closeness, intimacy and proximity as strong ties, or close friends, but who provide access to new information and diverse sets of social circles (see also Quan-Haase et al. 2002).

The data also show that respondents have *M*=5.31 (*S.D.*=11.37) 'friends' listed in their personal networks that they have only met on Facebook. While this might suggest that respondents are willing to accept friendship requests from strangers, the interview data showed that the majority of these individuals were friends-of-friends that had been added at the advice of a 'connecting individual'. The interview respondents mentioned had it not been for the recommendation of the connecting individual, they would not have accepted the request for friendship. In this way, the recommendation served as validation of the individual's trustworthiness and justification for their inclusion in the respondent's personal network.

A few respondents reported adding individuals that they had met on a Facebook group or, in the case of incoming first year students, connecting to individuals entering the same academic program. For this latter group of respondents, Facebook provided a means to get to know other first year students in their program prior to arriving on campus. The interview respondents, however, reported deleting these individuals shortly after commencing their studies. The reasons for deletion ranged from dissimilar interest to annoyance to a failure to meet the individuals in person. Moreover, these respondents noted that that they no longer accept friendship requests from people not met first in person.

4.2. INFORMATION REVELATION ON FACEBOOK

4.2.1. Information Indicated on Profile

Before testing hypotheses 1-3, an overview of the amount and types of personal information indicated on respondents' profiles is provided. Respondents were asked in the questionnaire to report which of several salient aspects (such as sexual orientation, political views, and current address) they included on their profile.

In line with previous research (Govani and Pashley 2006; Gross and Acquisti 2005; Tufekci 2008), the data show high levels of information revelation on Facebook. Indeed, an overwhelming 99.35 percent 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 percent), e-mail address (83.1

percent), birth date (92.2 percent), the current city or town in which they live (80.5 percent), and almost all respondents reported posting an image of themselves (98.7 percent) and photos of their friends (96.1 percent). By contrast, few respondents reported disclosing their physical address (7.9 percent), their cell phone number (10.5 percent) or their IM screen name (16 percent), thereby limiting the likelihood of individuals contacting or locating them outside of Facebook.

Figure 4-3 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 percent compared to 100 percent), email address (85.5 percent compared to 85 percent), relationship status (64.8 percent compared to 60 percent) and birth date (94.5 percent compared to 95 percent). The only items that showed differences were current address, $\chi2(1, N = 72) = 5.47, p < .05$, and political views, $\chi2(1,N = 72) = 13.29, p > .05$. Females were less like than males to reveal their current address and political views on their profiles.

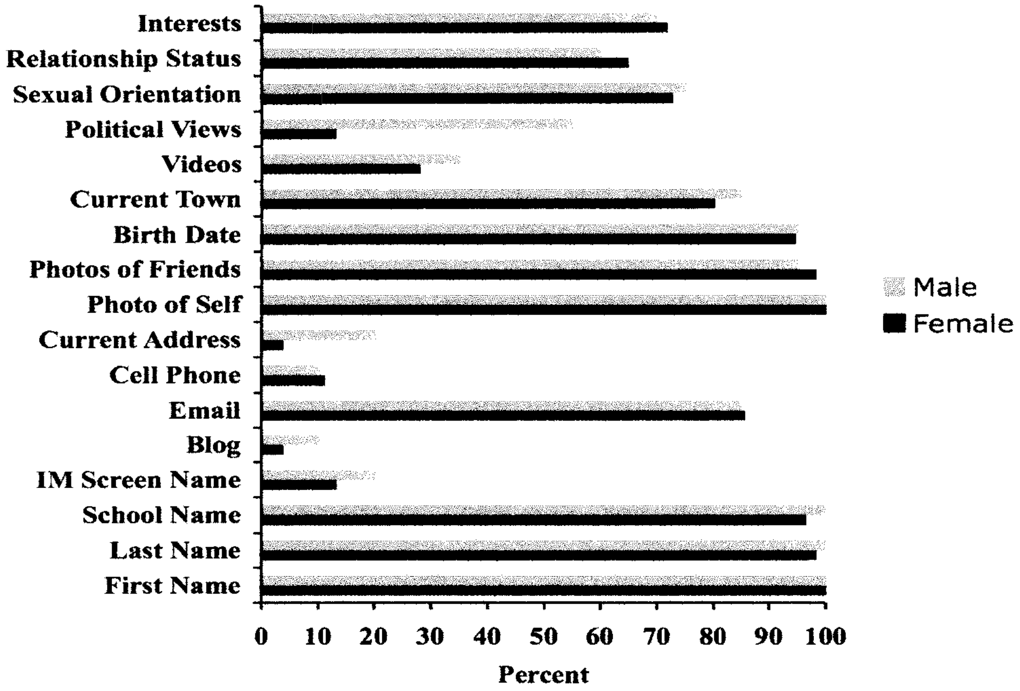


Figure 4-3. Information indicated on profile by gender

4.2.2. Privacy Concerns and Information Revelation

Hypothesis 1: Concern for Internet privacy will be negatively associated with information revelation on Facebook

Hypothesis 2: Concern about unwanted audiences will be negatively associated with information revelation on Facebook

To learn how Internet privacy and unwanted audience concerns relate to information revelation on Facebook, two separate correlations were conducted. The first correlation examined the relationship between general concern for Internet privacy and information revelation practices on Facebook. The second correlation analyzed the association between fear of unwanted audiences viewing undergraduate students' profile and the disclosure of personal information on Facebook. These analyses showed that concern for Internet privacy was negatively associated with information revelation on Facebook; the higher the concern, the less information revealed by respondents, $r(65) = -.26, p < .05$. By contrast, concern about unwanted audiences showed no effect, $r(64) = -.032, p = n.s.$ Thus, the data did support hypothesis 1, but did not support hypothesis 2.

As discussed in section 4.2.1 (p. 54), students generally reveal significant amounts of personal information on their profiles, including their full name, birth date, profile image, and photos of their friends. However, the data also shows that large percentages of students are apt to exclude their cell phone number and physical address from their profiles. The interview data provides some evidence for the exclusion of certain types of personal information based on respondents' general concern for Internet privacy. For example, Justine, a 3rd year science major, reported excluding her phone number, address, year of birth and residence information in order to manage her Internet privacy concerns. She reported that she did not disclose any information on the Internet that could be used to physically or financially harm her. The majority of interview respondents expressed similar comments around their disclosure of personal information on Facebook and their general concerns for Internet privacy. Thus, the interview data suggest that students' concern for Internet privacy factors into their information revelation on Facebook.

4.2.3. Impact of Network Size on Information Revelation

Hypothesis 3: Network size will be positively associated with information revelation on Facebook

In hypothesis 3, an association was hypothesized between the size of students' personal networks and the amount of information revealed. To test this prediction, a correlation was conducted with the participants' personal network size and the amount of information revealed as the variables. Results for this analysis showed a correlation between network size and information revelation; the larger the students' personal networks, the more likely they were to reveal information on Facebook, $r(66) = .307, p < .05$. Thus, hypothesis 3 was supported; network size is positively associated with information revelation on Facebook.

4.2.4. Additional Factors Influencing Information Revelation on Facebook

Besides the three factors of information revelation discussed above, the interview data show three additional factors that influence undergraduate students' information revelation on Facebook. The first factor discussed by respondents was the desire to be found by their friends and peers in Facebook searches, which influenced them to post a profile image. Several respondents reported that the profile image connects the profile to the user and enables friends and peers to find them in Facebook searches. As one respondent, Andrew, a 2nd year music student noted, "How else are other people supposed to know whether or not to add me as a friend; there are thousands of people with the same name as me on Facebook." In this way, profile images serve as signals, enabling users to find and be found by their friends and peers, which, in turn, allows for friendship connections to be established on Facebook.

The second factor influencing respondents' information revelation on Facebook was whether or not they previously revealed the information 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.

Finally, the interview data also provide evidence for the exclusion of contact information. Several respondents reported that their decision to withhold contact information was influenced by their desire to reduce the likelihood of unwanted audiences finding them in a physical location. For example, when asked about her decision to exclude her phone number and physical address, one respondent, Justine, a 20-year-old science student, noted, "Because I don't want people to know too much about me. I don't want them calling me. If they really need to know me, they can Facebook me (i.e., send her a private Facebook message). I don't want strangers knowing what my phone number is and then look me up and find out where I live." Similar comments around concerns about the disclosure of contact information came from the majority of respondents, suggesting that undergraduate students see the disclosure of contact information to be potentially harmful and too private for inclusion on their profiles.

4.3. PRIVACY PROTECTION IN FACEBOOK

4.3.1. Profile Visibility

Before testing hypotheses 4 and 5, an analysis of respondents' profile visibility was conducted. Profile visibility was measured at two levels: outside profile visibility, which measured to whom respondents' profiles are currently visible, and inside profile visibility, which assessed whether respondents have restricted access to their information or left their information open to others. The data obtained from these measures were analyzed using descriptive statistics and the percentages were recorded in Figure 4-4 for Outside profile visibility (p. 59) and Table 4-3 for Inside profile visibility (p. 60).

Figure 4-4 shows that 64.5 percent 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 percent had opted to leave their profile open to 'anyone' searching the Facebook network. The data also reveals that nearly a quarter of respondents chose to either leave their profiles open to 'all networks and all friends' (14.5 percent) or 'some networks and all friends" (6.6 percent), thus affording all individuals within their designated networks access to their profiles.

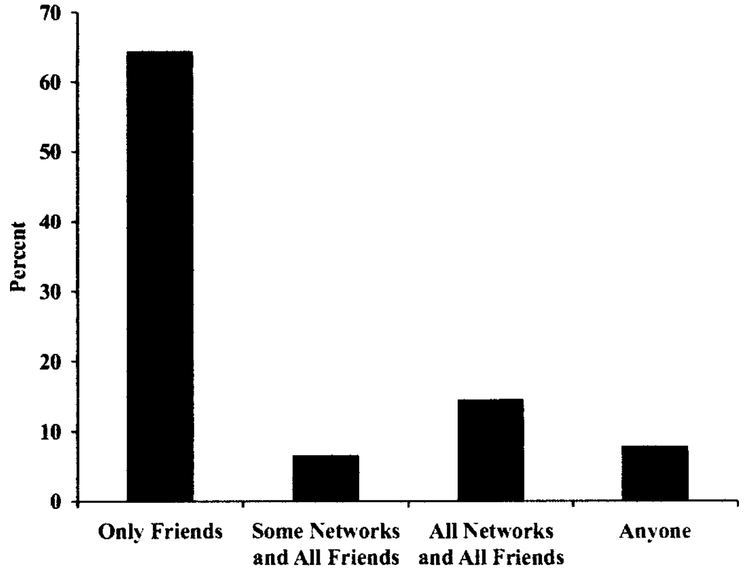


Figure 4-4. Outside profile visibility

Table 4-3 (p. 60) shows that large percentages of respondents have restricted the visibility of their information within Facebook. Indeed, 79.2 percent have restricted access to their tagged photos, 76.6 percent have restricted the visibility of their wall, and 71.4 percent have limited who can see their news feed/mini feed, which reports all activities undertaken by the user (e.g., adding or removing features, status updates, changes in relationship status, etc.). In addition, few students have left their list of friends (15.6 percent), list of courses (16.9 percent) and tagged videos (16.9 percent) open to unknown others.

Table 4-3 also shows that some respondents are unaware of the visibility of their information. For example, 23.4 percent and 20.8 percent reported that they are unsure about the visibility of their tagged photos and courses, respectively. A possible explanation for their inability to remember the visibility of their information may be that some respondents have not included this information on their profiles and therefore do not need to restrict access to the information.

Table 4-3 Inside profile visibility

Individual Items	Restricted Visibility		Open Visibility		Visibility Unknown	
	N	Percent	*N*	Percent	*N*	Percent
Tagged Photos	61	79.2	12	15.6	4	5.2
Tagged Videos	46	59.7	13	16.9	18	23.4
Status Updates	52	67.5	18	23.4	7	9.1
Online Status	52	67.5	17	22.1	8	10.4
Friends	49	63.6	12	15.6	10	13.0
Wall	59	76.6	15	19.5	3	3.9
Courses	48	62.3	13	16.9	16	20.8
News Feed/Mini Feed	55	71.4	12	15.6	10	13.0

4.3.2. Privacy Concerns and Profile Visibility

Hypothesis 4: Concern about unwanted audiences will be negatively associated with profile visibility on Facebook

Hypothesis 5: Concern for Internet privacy will be negatively associated with profile visibility on Facebook

To learn how concern for Internet privacy and concern about unwanted audiences relate to profile visibility, four correlations were conducted. The first correlation examined the relationship between general concern for Internet privacy and inside profile visibility – that is, to whom respondents' profiles are currently visible. The second correlation analyzed the association between concern about unwanted audiences and inside profile visibility. The third correlation investigated the relationship between general concern for Internet privacy and outside profile visibility – that is, whether or not respondents' information is currently visible. The fourth correlation examined the association between concern about unwanted audiences and outside profile visibility. These analyses showed that concern about unwanted audiences was negatively associated with inside profile visibility; the greater the concern, the less visible respondents' information, $r(48) = -.307, p < .05$. By contrast, the analyses showed no effect of concern for Internet privacy on outside profile visibility, $r(70) = -.146, p = n.s.$, or inside profile visibility, $r(69) = -.074, p = n.s.$, and no association between concern about unwanted audiences and outside profile visibility, $r(48) = -.235, p = n.s.$ Thus, hypothesis 4 was partially supported; concern about unwanted audiences was negatively associated with inside profile visibility, but not with outside profile visibility. Hypothesis 5 was refuted.

These results are somewhat surprising, especially considering that recent research has found that students typically manage their concerns about unwanted audiences by altering the visibility of their profile to 'only friends' (Tufekci 2008). These results may suggest that restricting the visibility of one's profile has become the norm for most students and that what is really important is how they handle the visibility of their information from within the site. Interviews in conjunction with the study suggest that while students are generally aware of the privacy risks associated with Facebook, they are not necessarily concerned about the possibility of unwanted audiences because they have enacted strict privacy settings, thereby reducing the chances of unwanted audiences accessing their profiles. A few respondents in the interview sample, however, noted that in the event that unwanted audiences are able to gain access to their profile, despite restricting their outside visibility to 'only friends,' they have also restricted access to certain types of personal information from within their profiles. For example, Cheryl, an 18-year-old social science student, noted that she changed the visibility of her uploaded and tagged photographs to 'only me' to further protect herself against the possibility of unwanted audiences. She explains,

> I'd rather censor pictures that people see of me. I mean if there is one of me doing something bad like drinking underage, I'd like to be able to make sure that I don't have that on in case other people can see my profile. I know that people say that employers can see it and stuff, so just in case. Even though [my profile is] private, I'd rather be safe than sorry.

From this comment, we begin to see that some students fear that despite restricting the visibility of their profile to 'only friends', unwanted audiences may still be able to access their profiles and the information within. To further protect herself against this possibility, Cheryl notes that she does not allow others to see her uploaded or tagged photographs.

The interview data also showed that concern for Internet privacy did not appear to have an effect on respondents' outside profile visibility; despite their level of concern, respondents were equally likely to have changed the visibility of their profile to 'only friends' as they were to have left their profile open to 'all of their networks and all of their friends' or 'some of their networks and all of their friends'. Thus, the data suggest that students manage unwanted audience concerns by altering the visibility of their information from within Facebook in addition to restricting access to their profiles, which appears to have become the norm for most students. The findings also show no relationship between Internet privacy concerns and students' level of outside profile visibility.

4.3.3. Use of Privacy Protection Strategies

To further investigate the strategies that undergraduate students have developed to protect themselves against privacy threats while using Facebook, respondents were asked in the questionnaire to indicate whether or not they have employed a variety of privacy protection strategies. Table 4-4 (p. 63) shows that the privacy protection strategies employed most often by undergraduate students are the exclusion of personal information to restrict unwanted audiences from obtaining certain information about themselves (*M*=4.08; *S.D.*=1.17), the use of private email messages within Facebook to restrict others from viewing the content of the message (*M*=4.72; *S.D.*=0.68), and altering Facebook's default privacy settings (*M*=4.33; *S.D.*=1.25). These strategies are followed by students' use of the limited profile (*M*=3.47; *S.D.*=1.70), which enables users to restrict certain contacts from viewing various aspects of their profile (such as photos, the wall, and work information), the deletion of wall posts to restrict others from viewing/reading the message (*M*=3.64; *S.D.*=1.55), and untagging one's self from photos and/or videos posted by their contacts (*M*=3.85; *S.D.*=1.55). By contrast, students do not use fake or inaccurate information to restrict unwanted audiences from obtaining personal information (*M*=1.66; *S.D.*=1.03) and very rarely block former contacts to restrict them from accessing their profile and engaging in conversation (*M*=2.91; *S.D.*=1.71).

Table 4-4 Privacy protection on Facebook

Individual Items and Scale	***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

The interview data provide insight into the reasons why undergraduate students employ certain privacy protection strategies and not others. The data show that each strategy has unique characteristics and therefore supports undergraduate students' privacy protection objectives in different ways. These objectives can best be understood in terms of expressive privacy concerns and informational privacy concerns, which have been described, as discussed in the literature review, by Goldie (2006) as the ability to control the extent to which an individual is known by chosen others and the right to control access to one's personal information (e.g., financial and medical records), respectively (see also DeCew 1997; Westin 1972).

Expressive Privacy Concerns

The first group of privacy concerns discussed by respondents most closely reflected expressive privacy. An expressive privacy concern, for example, is that certain individuals known to the Facebook user in an offline context will stumble on the user's postings, images, or information. As one respondent, Christine, a 1st 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 become 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 protective measures to protect herself against subsequent negative feedback from her family (i.e., the removal and untagging of photographs that depict her in questionable activities). In other words, the respondent has opted to limit her self-expression in order to reduce the likelihood of family members accessing content that they might deem inappropriate. In the context of this study, the concept of limiting one's self-expression was used to refer to censoring one's personal data on Facebook to avoid potential criticism from known others, and is distinct from limiting one's self-expression because of fear of persecution or physical harm due to one's choice of dress, religious affiliation, personal values and beliefs, etc.

Use of the limited profile was another measure employed by respondents to protect their expressive privacy. The limited profile enables users to restrict certain groups of individuals from accessing various types of information, such as tagged photos, online status, and work information, contained on the user's profile. For example, Justine, a 3rd year science student, reported that she had placed her sister and their mutual friends on a limited profile in order to restrict them from accessing information that could subsequently be used to inform her mother of her activities. In this way, use of the limited profile, instead of untagging and excluding certain types of photographs, enabled Justine and others to protect their expressive privacy without significantly limiting their self-expression and freedom to associate.

Informational Privacy Concerns

Despite the mention of expressive privacy concerns, it was the informational privacy concerns that respondents faced when using Facebook that appeared to be the most pressing and the most in need of protection. An informational privacy concern, for example, is that unwanted audiences will be able to access the information disclosed and use it for purposes to harm the individual. As one respondent, Rebecca, a 22-year-old humanities student, 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 reduce the likelihood of unwanted audiences "hunting her down", Rebecca has enacted various protective measures. First, she has changed her profile visibility to 'only friends' to restrict individuals external to her Facebook network from accessing her profile. Second, she has opted to use a profile image that shows only half her face. Her decision to use a semi-concealed photo was to dissuade unwanted audiences from contacting her or using the photo to locate her in an offline context. She also notes that the photo is recognizable enough that people known to her would be able to identify her face in the photo and subsequently be able to add her to their Facebook network if they were so inclined. Third, she has excluded all contact information, such as her phone number and physical address, to further reduce the chances of unwanted audiences locating her in an offline context. Finally, she has falsified the name of her hometown; in its place she has opted to use "Boonies, Ontario". As the name suggests, she is from a small town in rural Ontario – one in which it would be easy for an individual to locate her if they had both her name and the actual name of her hometown. Thus, she has decided to falsify the name of her hometown to even further reduce her chances of being found in an offline context by unwanted audiences.

Similar comments around concerns about unwanted audiences came from the majority of the respondents. Another respondent, Cheryl, an 18-year-old social science student, for example, noted that her primary concern with Facebook centers on the threat of stalkers and, to a lesser extent, future employers accessing her profile and using the information to harm her. To protect herself against the possibility of unwanted audiences, Cheryl noted that she has enacted a few protective measures, including restricting access to her profile to 'friends only' and withholding certain types of personal information, such as contact information (e.g., current address and landline phone number) that could be used to link her to a physical location. Moreover, she noted that she censors the types of photos that she posts to her profile. For example, she will not post images that depict her engaged in underage drinking.

In addition to the informational privacy risks posed by unwanted audiences accessing the information contained on Facebook profiles and using it to locate and/or harm the individual, a few respondents noted that their primary concern with Facebook is that their information will be used or appropriated for a variety of purposes without their consent. As one respondent, Melinda, a 4th year humanities student, noted:

> 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, and I find when friends post their writing or whatever the only thing that I comment is: "Facebook owns this, just so you know." And like I said, I don't put anything on there that you wouldn't be able to find out somewhere else.

From this comment, we begin to see that some students are aware of how their personal information and postings could be used or appropriated for purposes other than those initially intended by the user. To protect her information and intellectual property, Melinda notes that she does not post anything that could not be found somewhere else or which she does not want to become the property of Facebook. In this way, Melinda's primary protective strategy on Facebook is to disclose as little as possible.

Fake or Inaccurate Information

The interview data also provide evidence as to why undergraduate students tend to avoid the use of fake or inaccurate information as a protective measure. The primary reason expressed by the sample was that it seemed ridiculous to use falsified information because their friends would question the validity of the information disclosed. Moreover, a few respondents mentioned that their use of untrue information in the past, such as indicating a change in relationship status from, for example, 'in a relationship' to 'engaged' or 'married', had caused confusion and had resulted in numerous messages inquiring about the change in status. Thus, to avoid any further confusion or backlash, these respondents noted that they no longer use fake or inaccurate information on their profiles.

While the majority of respondents opted to include only factual information on their profile, a few respondents noted that their 'about me' section was in fact fictional. These respondents, however, indicated that the information was intended to be comical rather than intentionally deceitful. For example, Charlie, a 4th year science student, reported that instead of posting truthful information about himself, he opted to use a humorous passage that he found on a Web site. He explains, "I have an affinity for laughter and I wish to make anyone who reads my [about me] section [to] laugh. I assume that they know I could not have possibly accomplished all those things that I have written." 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).

4.3.4. Use of Communication Tools

An examination of the communication practices employed by respondents provides further insight into the privacy protection strategies of undergraduate students. While the data showed that students use the wall (96.1 percent) as often as they used private emails (95 percent), information obtained from the interviews revealed that each communication tool serves a specific purpose and supports students' communication and privacy objectives in different ways. The data suggest that the wall is used most often when students are unconcerned if others view or gain access to their postings, and that private Facebook emails are reserved for messages that contain personal or private information, such as a phone number or physical address. In this way, students manage the boundary between public and private by posting public messages to the wall and sending confidential information via private emails.

4.4. SUMMARY

This chapter presented the analyses and results for hypothesis 1-5. The analyses showed that students manage their concerns for Internet privacy by withholding personal information from their profiles and address their concerns about unwanted audiences by altering the visibility of their information from within Facebook. Furthermore, an examination of the relationship between information revelation and network size revealed that students who disclose more information on Facebook also tend to have larger personal networks. Table 4-5 (p. 68) provides a summary of the findings.

Table 4-5 Summary of findings

Hypotheses	Supported	Partially supported	Not supported
H1: Concern for Internet privacy will be negatively associated with information revelation on Facebook	X		
H2: Concern about unwanted audiences will be negatively associated with information revelation on Facebook			X
H3: Network size will be positively associated with information revelation on Facebook	X		
H4: Concern about unwanted audiences will be negatively associated with profile visibility		X	
H5: Concern for Internet privacy will be negatively associated with profile visibility			X

CHAPTER 5
CONCLUSIONS

5.1. DISCUSSION

As in previous research (Acquisti and Gross 2006; Govani and Pashley 2006; Gross and Acquisti 2005; Tufekci 2008), the results of this study showed that students disclose considerable amounts of personal information and often use accurate personal information on their profiles. Indeed, the present study found that large percentages of students had revealed their real name (99.35 percent), school name (97.5 percent), birth date (92.2 percent) and a self-image (97.4 percent) on their profiles. By contrast, the present study found that students were less likely to reveal their cell phone number (10.5 percent) and physical address (7.9 percent) than indicated in previous research. For example, in a study examining information sharing and privacy on Facebook, Acquisti and Gross (2006) found that 39 percent and 24 percent of students had revealed their accurate cell phone number and physical address, respectively. These differences in findings may be the result of Facebook opening its doors to everyone in September 2006. Given that Acquisti and Gross (2006) studied student information revelation and privacy protection behaviors prior to Facebook's decision to allow general audiences to create profiles on the site, it is possible that since conducting their study students' information revelation practices have changed. This is not to suggest that students' information revelation practices have changed dramatically, but rather that they may have become more selective in the amount and types of information that they chose to disclose. For instance, while students' use of their cell phone number and physical address have declined, large percentages of students continue to disclose other types of personally-identifiable information, including those discussed above. As Tufekci (2008) has suggested, by allowing the general public to use Facebook, students' perceptions of Facebook as a secure and private community may have been altered, thus affecting their behaviors and information revelation practices on the site. In this way, many students may be more inclined to withhold certain types of personal information from their profiles than they were before the site was open to the general public.

In the present study I found that Internet privacy concerns have a greater impact on undergraduate students' information revelation practices than indicated in previous research (Acquisti and Gross 2006; Tufekci 2008). An examination of the relationship between concern for Internet privacy and the amount of information disclosed showed that students with a greater level of concern for Internet privacy disclosed less personal information on their profiles. Contrary to previous findings, the results of the present study suggest that students not only "say they are concerned" about privacy on the Internet, they also make concerted efforts to protect themselves against possible invasions by withholding personal information.

This is not to suggest, however, that students manage their Internet privacy concerns through complete withdrawal, but rather that they are selective in the amount and types of information that they chose to display. As other researchers have noted, SNS profiles have become a vehicle for identity performance and formation (boyd in press; Laraqui 2007), requiring a certain level of self-disclosure in order for them to be useful (Tufekci 2008). In interviews for the present study, many students expressed an awareness of the minimum level of self-presentation and information revelation required, indicating that it seems pointless to have a profile if it does not provide enough information about the user. In other words, just as one must devote a certain level of time and attention to the presentation of the self in order to engage in identity performance in physical space (Goffman 1959), one must also reveal a certain amount of personal information in order to exist online (Sundén 2003; see also Tufekci 2008). As Tufekci (2008) notes, the overwhelming adoption of SNSs by university students indicates that remaining "unlisted" is not a desirable option for students.

The nearly universal inclusion of real name, profile image and school name on students' profiles are examples of this minimum level of disclosure and self-presentation. While Facebook does not *require* users to use their real name, and profile images and school names are optional, large percentages of students chose to reveal this information on their profiles. Tufekci (2008) suggests that "online environments have cultural norms (which are different from each other) and certain *expectations* about levels of participation" (33). Interviews in conjunction with the present study suggest that many students understand the cultural norms of Facebook and see a certain level of disclosure as necessary to establish *common ground* and to reduce the *costs* associated with searching Facebook profiles. In this way, by revealing certain types of personal information, such as one's real name, profile image and school name, students make it easier for their friends and peers to find them on Facebook.

In the present study I also found that students' personal network size has an impact on their information revelation on Facebook: the more friends in students' personal network, the more information they were likely to reveal on their profiles. As Lampe, Ellison and Steinfield (2007) have noted, profile elements act as signals, which reveal personality aspects of the user and assist people in establishing *common ground* and making decisions about whether or not to declare friendship connections. Furthermore, they contend that in populating profile fields, such as location information (i.e., hometown, school name, current city, etc.), users effectively reduce the *costs* associated with searching SNS profiles, making it easier for current classmates, former high school friends or people located in the same university or college dormitory to find them in SNS searches. This, in turn, increases the chances that friendship connections will be established on these sites. In line with the findings of Lampe, Ellison and Steinfield (2007), the results of the present study suggest that higher levels of information revelation contribute to larger social networks on SNSs, which, in turn, increases students' opportunities for social interaction and participation, as well as for the maintenance and formation of relationships.

While students attempt to optimize their chances for publicity and social participation by disclosing information that can be used to assist their friends and peers in locating them, they also try to manage their privacy concerns by withholding certain types of personal information. An examination of the amount and types of information disclosed by respondents showed that only a small percentage of students had revealed their cell phone number and physical address. Interviews suggest that students perceive the disclosure of this type of information to be potentially harmful and therefore opt to exclude it from their profiles. Furthermore, several respondents reported sending contact and other confidential information in private Facebook emails, rather than posting the information to a friend's wall or revealing it on their profiles.

The findings of the study indicate that students address their concerns about unwanted audiences by altering the visibility of their information from within the site (inside profile visibility), but not by limiting the amount of personal information that they disclose (information revelation) or altering the visibility of their profiles (outside profile visibility). Interviews in conjunction with the present study suggest that although students are generally aware of the privacy implications associated with Facebook, the majority of students are not overly concerned because they have enacted restrictive privacy settings, thereby reducing the chances of unwanted audiences accessing their profiles. Indeed, 64.5 percent of respondents in the questionnaire sample reported changing their default settings to restrict other Facebook users not on their friends list from accessing their profiles. These results are inconsistent with previous research (Tufekci 2008), which has found that students typically manage their concerns about unwanted audiences by altering the visibility of their profile to 'only friends'. This may suggest that altering one's outside profile visibility – that is, the extent to which one's profile is accessible by other Facebook users – has become the norm for most students and what really matters is how they protect their inside profile visibility – that is, to whom their information is visible from within the site. The present study showed that large percentages of students had altered the visibility to their information from within, including who can see their tagged photos (79.2 percent), news feed/mini feed (71.4 percent), wall (76.6 percent) and online status (67.5 percent). Furthermore, in interviews a few students reported restricting access to certain types of personal information, such as photographs, in addition to altering the visibility of their profiles to 'only friends'. This examination of profile visibility is unique in that no other research to date has examined both types of profile visibility within a single study.

The results of the present also suggest that students employ a variety of privacy protection strategies in order to address their various privacy concerns. For example, students in the interview sample who expressed concerns related to expressive privacy (DeCew 1997; Goldie 2006) – that is, fear that individuals known to them in an offline context will stumble upon their postings, information, pictures, etc. – tended to manage their concerns by either untagging and removing photographs that depict them engaged in questionable activities or making use of the limited profile to restrict certain contacts or groups of contacts from viewing specific types of personal information. By contrast, students who expressed concerns related to informational privacy (Goldie 2006; Westin 1972) – that is, fear that unwanted audiences will access their personal information and use it for purposes to harm them – were apt to restrict access to their profile and the information contained within and to withhold information that could be used to link them to a physical location (e.g., physical address, landline phone number and residence information) or for data mining purposes. Thus, the data suggest that each privacy protection strategy has unique characteristics and therefore supports undergraduate students' privacy objectives in different ways.

It is interesting to note that undergraduate students do not perceive the use of fake or inaccurate information to be a useful protective measure. Indeed, interviews suggest that students consider the falsification of personal information to be impractical 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 in SNSs serves as verification on the reliability of one's identity claims, ensuring that profiles are kept honest and truthful or playful and ironic, rather than intentionally deceptive (Donath and boyd 2004; Lampe, Steinfield and Ellison 2007; see also Donath forthcoming 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 and honest in nature.

In sum, the results of this study revealed that students protect themselves against the possibility of unwanted audiences by adjusting the visibility of their information and they manage their concerns for Internet privacy by withholding certain types of personal information from their profiles (i.e., contact and other confidential information). They do not, however, use fake or inaccurate information as a protective measure because their friends and peers would question the validity of the information disclosed. As several respondents noted, they would rather not provide the information than lie. Furthermore, the results of the study suggest that students see a minimum level of self-presentation and information revelation as necessary to make Facebook useful. If being found on Facebook is a primary objective of students, then information such as one's real name, profile image and school name is necessary to assist their friends and peers in locating them. Therefore, students manage their privacy concerns not by complete withdrawal, as this would limit their chances for public display and social interaction, but rather by altering the visibility of their profile from within and excluding certain types of personally-identifiable information.

5.2. LIMITATIONS AND FUTURE RESEARCH

There were three primary methodological limitations of the present study, all of which reflect concerns related to the selection of the sample. The first limitation is that the sample was not random but rather based on convenience. That is, respondents were chosen based on ease of accessibility and availability to participate. This is problematic because the students selected may not be typical or representative of the larger undergraduate student population from which they have been chosen (Babbie 2002) and therefore inferences cannot adequately be made about the larger population. The second limitation is that the sample was relatively small. The present study relied on quantitative data from 77 participants and qualitative data from 21 respondents. This further limits the interpretability of the results by reducing the possibility of obtaining diversity and a range of opinions that reflect the larger population. To address these limitations, future research could seek to obtain a larger and more representative sample by employing a random or probability sampling technique. This would ensure that the same variations that exist in the population under study are represented in the sample. The third limitation is that the results of the study only apply to university students. Future research could seek to examine 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.

Besides these three methodological limitations resulting from the size, composition and selection of the sample, there was also an issue that arose from the examination of Facebook. The biggest concern with Facebook is that it is a changing technology; new features and settings are constantly added or updated to meet the demands and concerns of its users. For example, in March 2008 Facebook added additional privacy settings, which afford users more control over the information that they chose to post to their profiles, including the ability to share and restrict access to their information based on specific friends and friend lists. These settings replaced the limited profile, which enabled users to restrict certain individuals from seeing a specified set of information. In other words, all individuals set to a limited profile were restricted from seeing the same types of information. The inclusion of these new features and settings, however, is problematic because the features of Facebook examined at one point in time may not be the same features employed by users at another point in time. In terms of the present study, the additional privacy controls mentioned above were added following data collection in October and November 2007. This means that the privacy settings employed by respondents during data collection may have changed following the inclusion of the new privacy controls. Thus, the results of the present study may not reflect undergraduate students' information revelation and privacy protection practices on Facebook at this point in time. Future research therefore could seek to determine how the inclusion of these additional privacy controls has changed the way that undergraduate students protect their privacy when using Facebook and how they decide what information to reveal and what to conceal on their profiles.

References

Acquisti, Alessandro and Ralph Gross. 2006. Imagined communities: awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technologies*, 36-58. Springer.

Adler, Ron and Neil Towne. 1999. *Looking out/looking in: Interpersonal communication.* 9th ed. San Francisco: Harcourt Brace.

Altman, Irwin. 1975. *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, California: Brooks/Cole Publishing.

Augustinas, Sarah J. 2005. Universities monitor Facebook posts, photos. *Northern Star (Northern Illinois)*. November 23. http://media.www.dailycollegian.com/media/storage/paper874/news/2005/11/23/News/Universities.Monitor.Facebook.Posts.Photos-1561190.shtml (accessed November 2, 2007).

Axinn, William G. and Lisa D. Pearce. 2006. *Mixed method data collection strategies*. New York: Cambridge University Press.

Babbie, Earl and Lucia Benaquisto. 2002. *Fundamentals of social research.* 1st Canadian ed. Canada: Nelson Education Ltd.

Babbie, Earl. 2002. *The basics of social research.* 2nd ed. Canada: Wadsworth.

Barnes, Susan B. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11, no. 9 http://www.firstmonday.org/issues/issue11_9/barnes/index.html (accessed July 17, 2007).

boyd, danah and Nicole Ellison. 2007. History of social network sites. *Journal of Computer-Mediated Communication* 13, no. 1 (October) http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (accessed November 2, 2007).

boyd, danah and Jeffrey Heer. 2006. Profiles as conversations: Networked identity performance on Friendster. In *Proceedings of the Hawai'I International Conference on System Sciences (HICSS-39)*, Persistent Conversation Track.

Kauai, HI: IEEE Computer Society (January 4-7). http://www/danah.org/papers/HICSS2006.pdf (accessed August 21, 2007).

boyd, danah and Henry Jenkins. 2006. MySpace and Deleting Online Predators Act (DOPA). *MIT Tech Talks*, May 26. http://www.danah.org/papers/MySpaceDOPA.html (accessed August 15, 2007).

boyd, danah. 2006a. Friends, Friendsters, and MySpace Top 8: Writing community into being on social network sites. *First Monday* 11, no. 12 (December). http://www.dahan.org/papers/FriendsFriendsterTop8.pdf (accessed October 22, 2007).

boyd, danah. 2006b. Friendster lost steam. Is MySpace just a fad? *Apophenia Blog*. http://www.danah.org/papers/FriendsterMySpaceEsay.html (accessed October 23, 2007).

boyd, danah. 2004. Friendster and publically articulated social networking. *Conference on Human Factors and Computing Systems (CHI 2004)*. Vienna: ACM Press, April 24-29, 2004. http://www.danah.org/papers/CHI2004Friendster.pdf (accessed October 21, 2007).

boyd, danah. 2007. Social network sites: Public, private, or what? *Knowledge Tree* (May). http://www.danah.org.papers.KnowledgeTree.pdf (accessed August 20, 2007).

boyd, danah. in press. Why youth (heart) social networking sites: The role of networked publics in teenage social life. In *The MacArthur Foundation Series on Digital Learning, Identity Volume*. Ed. David Buckingham. MIT Press. http://www.danah.org/papers/WhyYouthHeart.pdf (accessed August 22, 2007).

Brown, Louise. 2008a. Student faces Facebook consequences: Freshman hit with 147 academic charges for online study network at Ryerson University. *The Star.com*, March 6. http://www.thestar.com/News/GTA/article/309855 (accessed March 27, 2008).

Brown, Louise. 2008b. Facebook user can stay at Ryerson: Engineering student ducks expulsion for running shared-homework site. *The Star.com*, March 19. http://www.thestar.com/News/GTA/article/347688 (accessed March 27, 2008).

Bryman, Alan, and James J. Teevan. *Social research methods*. Canadian edition. Canada: Oxford University Press.

Buckman, Rebecca. 2005. Too much information?; Colleges fear student postings on popular 'Facebook' site could pose security risks. *The Wall Street Journal (Eastern Edition)*. New York, N.Y.: December 8, B1.

CBS Evening News. 2006. Employers look at Facebook, too. *CBS*, June 20. http:///www/cbsnews.com/stories/2006/06/20/eveningnews/main1734920.shtml?source=search_story (accessed August 5, 2007).

Chapman, Scott and Gurpreet S. Dhillon. 2002. Privacy and the Internet: The case of DoubleClick, Inc. In *Social Responsibility in the Information Age: Issues and Controversies*, ed. Gurpreet Dhillion, 75-88. Hershey, PA: Idea Group Publishing.

comScore Networks. 2007. Social networking goes global. *comScore*, July 31 http://www.comscore.com/press/release.asp?press=1555 (accessed October 25, 2007).

Coser, Rose Laub. 1975. The complexity of roles as a seedbed of individual autonomy. In *The Idea of Social Structure: Papers in Honor of Robert K. Merton*, ed. Lewis A. Coser. 237-262, New York, NY: Harcourt Brace Jovanovich.

Culnan, Mary J, 2000. Protecting privacy online: Is self-regulation working? *Journal of Public Policy and Marketing* 19, no. 1 (Spring): 20-26.

Creswell, John W. 2003. *Research design: Qualitative, quantitative, and mixed methods approaches*. 2nd ed. Thousand Oaks: Sage Publications.

Creswell, John W. and Vicki L. Plano Clark. 2007. *Designing and conducting mixed methods research*. Thousand Oaks: Sage Publications.

DeCew, Judith Wagner. 1997. *In pursuit of privacy: Law, ethics & the rise of technology*. Ithaca: Cornell University Press.

de Vaus, D.A. 1995. *Surveys in social research.* 4th ed. Australia: Allen & Unwin.

Dillman, Don. A. 1978. *Mail and telephone surveys: The total design method.* Toronto: John Wiley & Sons.

Dillman, Don A, Glenn Phelps, Robert Tortora, Karen Swift, Julie Kohrell, and Jodi Berck. 2008. Response rate and measurement differences in mixed mode surveys using mail, telephone, interactive voice response and the Internet. http://www.jstor.org.proxy1.lib.uwo.ca:2048/stable/pdfplus/2749203.pdf (accessed May 11, 2008).

Donath, Judith and danah boyd. 2004. Public displays of connection. *BT Technology Journal* 22, no. 4: 71-82.

Foucault, Michel. 1979. *Discipline and punish: The birth of the prison.* New York: Vintage Books.

Goffman, Erving. 1959. *The presentation of self in everyday life.* New York: Doubleday Anchor Books.

Goldie, Janis L. 2006. Virtual communities and the social dimension of privacy. *University of Ottawa Technology and Law Journal* 3, no. 1: 133-167

Goldsmith, Jack and Tim Wu. 2006. *Who controls the Internet?: Illusions of a borderless world.* New York: Oxford University Press

Govani, Tabreez and Harriet Pashley. 2006. Student awareness of the privacy implications when using Facebook. November 21. http://lorrie.cranor.org/courses/fao5/tubzhl.pdf (accessed July 15, 2007).

Gross, Ralph and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society.* Alexandria, VA: ACM Press, November 7, 2005.

Henderson, Sandra C., Charles A. Synder, and Terry Anthony Byrd. 2002. Electronic commerce and data privacy: The impact of privacy concerns on electronic commerce use and regulatory preferences. In *Social Responsibility in the*

Information Age: Issues and Controversies, ed. Gurpreet Dhillon. 89-113, Hershey, PA: Idea Group Publishing.

Hitwise.com. 2008. MySpace received 76 percent of U.S. social networking visits in 2007. *Hitwise*, January 16 http://www.hitwise.com/press-center/hitwiseHS2004/social-networking-visits-in-2007.php (accessed March 27, 2008).

Jones, Harvey and Jose Hiram Soltren. 2005. Facebook: Threats to privacy http://www.swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf (accessed August 7, 2007).

Jones, K.C. 2007. Oxford University fines students for Facebook 'flour' photos. *Information Week.* July 17 http://www.informationweek.com/internet/showArticle.jhtml?articleID=201001822 (accessed November 2, 2007).

Klein, Julie. 2006. Schools use Facebook for admissions, disciplinary action. *The Stanford Daily*, February 14 http:///daily.stanford.edu/article/2006/2/14/schoolsUseFacebookForAdmissionsDisciplinaryAction (accessed August 5, 2007).

Lampe, Cliff A. C., Nicole Ellison, and Charles Steinfield. 2007. A familiar Face(book): Profile elements as signals in an online social network. In *Proceedings of the SIGCHI conference on Human factors in computing systems.* San Jose, California: ACM Press, April 28-May 3, 2007.

Laraqui, Jawad. 2007. Activity based interfaces in online social networks. Masters Thesis, Massachusetts Institute of Technology (MIT) http://smg.medis/mit.edu/papers/laraqui_thesis.pdf (accessed November 4, 2007).

Legard, Robin, Jill Keegan, and Kit Ward. 2003. In-depth interviews. In *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, eds. Jane Ritchie and Jane Lewis, 138-169. Thousand Oaks, CA: Sage Publications.

Lenhart, Amanda and Mary Madden. 2007. Teens, privacy & online social networks: How teens manage their online identities and personal information in the age of MySpace. *PEW Internet and American Life Project*. Washington, D.C. (April 18). http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf (accessed August 25, 2007).

Margulis, Stephen T. 2003a. On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues* 59, no. 2: 411-429.

Margulis, Stephen T. 2003b. Privacy as a social issue and behavioral concept. *Journal of Social Issues* 59, no, 2: 243-261.

Marx, Gary T. 1999. Privacy and technology (Revised material that appeared in *The World and I*, September 1990 and *Telektronik* January 1996) [Online] http://web.mit.edu/gtmarx/www/privantt.html (accessed October 31, 2007).

Metzger, Miriam J. 2007. Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication* 12: 1-27.

Michaels, Tim. 2006. Future employers may consider Facebook profiles. *Chicago Maroon*, April 18 http://maroon.uchicago.edu/news/articles/2006/04/08/future_employers_may.php (accessed August 5, 2007).

Mizes, J. Scott, E. Louis Fleece, and Cindy Roos. 1984. Incentives for increasing return rates: Magnitude levels, response bias, and format. *The Public Opinion Quarterly* 48, no. 4 (Winter): 794-800.

Needham and Company. 2007. YAHOO: Yahoo! may regret not paying up for Facebook. *Needham and Company* http://www.needhamco.com/Research/Documents/CPY25924.pdf (accessed October 25, 2007)

O'Neil, Dara. 2001. Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review* 19, no. 1 (Spring): 17-31.

Panja, Tariq. 2007. Oxford using Facebook to snoop. *Associated Press*. July 17 http://www.msnbc.msn.com/id/19813092/ (accessed November 2, 2007).

Peters, Thomas A. 1999. *Computerized monitoring and online privacy*. Jefferson, NC: McFarland & Company, Inc.

Pew Internet and American Life Project. 2000. Trust and privacy online: Why Americans want to rewrite the rules. *PEW*. http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf Accessed April 4, 2008.

Quan-Haase, Anabel, Barry Wellman, James Witt, and Keith Hampton. 2002. Capitalizing on the Internet: Social contact, civic engagement, and sense of community. In *Internet and everyday life*, eds. Barry Wellman and Caroline Haythornthwaite, 291-324. London, U.K: Blackwell.

Ritchie, Jane, Liz Spencer, and William O'Connor. 2003. Carrying out qualitative analysis. In *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, eds. Jane Ritchie and Jane Lewis, 219-262. Thousand Oaks, CA: Sage Publications.

Ryze.com. 2007. http://www.ryze.com (accessed October 22, 2007).

Simmel, Arnold. 1971. Privacy is not an isolated freedom, In *Privacy*, ed. J. Roland Pennock and John W, Chapman, 71-87. New York: Atherton Press.

Solove, Daniel J. 2004. *The digital person: Technology and privacy in the information age*. New York: New York University Press.

Strater, Katherine and Heather Richter. 2007. Examining privacy and disclosure in a social networking community. *ACM International Conference Proceeding Series: Proceedings of the 3rd symposium on usable privacy and security*. ACM Press, Pittsburgh, PA, July 18-20, 2007.

Sundén, Jenny. 2003. *Material Virtualities: approaching online textual embodiment*. New York: Peter Lang.

Tashakkori, Abbas and Charles Teddlie. 1998. *Mixed methodology: Combining qualitative and quantitative approaches*. Thousand Oaks, California: Sage.

Tufekci, Zeynep. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology and Society*, 28, no. 20 (January): 20-36.

Viseu, Ana, Andrew Clement, and Jane Aspinall. 2004. Situating privacy online: Complex perceptions and everyday practices. *Information, Communication & Society* 7, no. 1 (March): 92-114.

Wellman, Barry, Janet Salaff, Dimitrina Dimitrova, Laura Garton, Milena Gulia, and Caroline Haythornthwaite. 1996. Computer networks as social networks: Collaborative work, telework, and virtual community. *Annual Review of Sociology*, 22: 213-239.

Westin, Alan F. 1972. *Databanks in a free society: Computers, record-keeping and privacy*. New York: Quadrangle Books

Westin, Alan F. 1967. *Freedom and privacy*. New York: Atheneum.

Westin, Alan F. 2003. Social and political dimensions of privacy. *Journal of Social Issues* 59, no. 2: 431-453.

Appendix A. Information Letter to Questionnaire Participants

Defacing the 'Book:
Understanding Student Self-Disclosure and Privacy Practices on Facebook
Alyson Young (Candidate for MA in Media Studies)
Thesis Supervisor: Dr. Anabel Quan-Haase (M.A., Ph.D.)

The purpose of this letter is to provide you with the information you require to make an informed decision on participating in this research. I am a Masters student in Media Studies in the Faculty of Information and Media Studies at the University of Western Ontario and the information I am collecting will be used in my thesis. If you decide not to participate in the study, this will not have negative consequences for the progression of my degree.

Purpose of this Study

You are being invited to participate in a research study looking at student self-disclosure and privacy practices on Facebook. This study investigates the reasons why undergraduate students disclose personal information on Facebook, and the way(s) they deal with privacy concerns while using the technology.

Who is eligible to Participate?

You are eligible to participate if you are enrolled in an undergraduate program at the University of Western Ontario.

Research Procedure of this Study

You will be asked to complete a paper-and-pencil based survey lasting approximately 15 minutes. We are planning to survey approximately 90 students at the University of Western Ontario. The study will take place in North Campus Building room 114.

Voluntary Participation

Participation in this study is voluntary. You may refuse to participate, refuse to answer any questions or withdraw from the study at any time with no effect on your future academic status.

Inquiries and Risks

You are free to ask questions about the study or survey at any time. There are no known risks involved from participating in this study. Participating in the present study does not hinder your ability to participate in concurrent studies or in future studies.

Benefits from the Study

There are no known benefits to you from participating in this study. However, your participation will help gain new insight and knowledge into the reasons why undergraduate students self-disclose on Facebook, as well as the way(s) they protect themselves while interacting with the technology.

Confidentiality of Information

Information that is collected during the study will either be stored in a locked cabinet or in a secure database on a secure server accessible only by the researchers (Alyson Young and Anabel Quan-Haase). Results of the study will be available from the researchers when the study is completed. If the results of the study are published, your name will not be used and no information that discloses your identity will be released or published. All records will be kept by Dr. Anabel Quan-Haase for educational purposes.

Compensation

In recognition of your contribution to this project, you will be given the opportunity to choose whether or not you would like to be entered into a draw for a chance to win one of four Tim Hortons' gift certificates valued at $10 each. Any additional costs you may incur as a result of your participation will not be reimbursed.

Consent to Participate

You consent to participate in the present study by completing the survey.

Contact

If you have any questions about this study, please contact:

Alyson Young, Masters Candidate
Graduate Program in Media Studies
Faculty of Information and Media Studies, The University of Western Ontario
Faculty Thesis Supervisor: Anabel Quan-Haase

If you have any questions about the conduct of this study or your rights as a research subject, you may contact:

The Director
Office of Research Ethics
The University of Western Ontario

Appendix B. Information Letter to Interview Participants

Defacing the 'Book: Understanding Student Self-Disclosure and Privacy Practices on Facebook
Alyson Young (Candidate for MA in Media Studies)
Thesis Supervisor: Dr. Anabel Quan-Haase (M.A., Ph.D.)

The purpose of this letter is to provide you with the information you require to make an informed decision on participating in this research. I am a Masters student in Media Studies in the Faculty of Information and Media Studies at the University of Western Ontario and the information I am collecting will be used in my thesis. If you decide not to participate in the study, this will not have negative consequences for the progression of my degree.

Purpose of this Study

You are being invited to participate in a research study looking at student self-disclosure and privacy practices on Facebook. This study investigates the reasons why undergraduate students disclose personal information on Facebook, and the way(s) they deal with privacy concerns while using the technology.

Who is eligible to Participate?

You are eligible to participate if you are enrolled in an undergraduate program at the University of Western Ontario.

Research Procedure of this Study

You will be asked to participate in an interview lasting approximately 30 minutes. We are planning to interview approximately 10 undergraduate students at the University of Western Ontario. The study will take place in one of the meeting rooms in the North Campus Building. During the interviews, students will be asked to show the researcher their Facebook site, and to discuss the reasons why they self-disclose on Facebook and how they deal with privacy concerns. The interviews will be audio taped, with the consent of the participants, and transcribed and analyzed in NVIVO.

Voluntary Participation

Participation in this study is voluntary. You may refuse to participate, refuse to answer any questions or withdraw from the study at any time with no effect on your future academic status.

Inquiries and Risks

You are free to ask questions about the study or survey at any time. There are no known risks involved from participating in this study. Participating in the present study does not hinder your ability to participate in concurrent studies or in future studies.

Benefits from the Study

There are no known benefits to you from participating in this study. However, your participation will help gain new insight and knowledge into the reasons why undergraduate students self-disclose on Facebook, as well as the way(s) they protect themselves while interacting with the technology. You do not waive any legal rights by signing this consent form.

Confidentiality of Information

Information that is collected during the study will be stored either in a locked cabinet or in a secure database on a secure server accessible only by the researchers (Alyson Young and Dr. Anabel Quan-Haase). The interviews will be audio taped, with your consent, and will be labeled with pseudonyms to ensure your confidentiality and anonymity. If the results of the study are published, your name will not be used and no information that discloses your identity will be released or published. Quotes from the interviews may be used in publications and reports; however, your name will not be associated with any of these quotes and no quotes will be disclosed that identify you or anybody else. All records will be kept by Dr. Anabel Quan-Haase for educational purposes.

Compensation

In recognition of your contribution to this project you will be given $10. Any additional costs you may incur as a result of your participation will not be reimbursed.

Contact

If you have any questions about this study, please contact:

Alyson Young, Masters Candidate
Graduate Program in Media Studies
Faculty of Information and Media Studies, The University of Western Ontario
Faculty Thesis Supervisor: Anabel Quan-Haase

If you have any questions about the conduct of this study or your rights as a research subject, you may contact:

The Director
Office of Research Ethics
The University of Western Ontario

Appendix C. Consent to be Interviewed

Defacing the 'Book: Understanding Student Self-Disclosure and Privacy Practices on Facebook

Consent Form

I have read the Information Letter, have had the nature of the study explained to me and I agree to participate in the study. All questions have been answered to my satisfaction.

Do you consent to be interviewed? Yes □ No □

Do you consent to be audio taped? Yes □ No □

____

Name (please print)

________________________________ ________________

Participant's Signature **Date**

____

Name of person obtaining informed consent (please print)

____________________________________ ________________

Signature of person obtaining informed consent **Date**

Appendix D. Paper-and-Pencil Based Questionnaire

Defacing the 'Book:
Understanding Student Self-Disclosure and Privacy Practices on Facebook

Alyson Young (Candidate for MA in Media Studies)
Thesis Supervisor: Dr. Anabel Quan-Haase (M.A., Ph.D.)

Instructions:

Please read the following questions carefully. Put an 'X' in the box or 'circle' the adequate response. You can use either pencil or pen. Once completed, please bring the survey back to class and place in the box labeled "COMPLETED SURVEYS" which will be located at the front of the classroom.

PART A:

Q1. How often do you visit Facebook?

Several times a day □
Once a day □
Several times a week □
Once a week □
Several times a month □
Once a month □
A couple of times a year □
Never □
Don't know/Refused □

If you do not use Facebook, please skip to Part B Question 9

Q2. On average, how much time did you spent on Facebook last week?

□ Hours □ Minutes

Q3. Approximately, when did you start using Facebook?

□ Year □ Month

Q4. What was your primary motivation(s) for **joining** Facebook?

Check all that apply

Friend suggested it □

Received a promotional e-mail □

Everyone I know is on Facebook □

Find classmates □

Find course information □

Find people with mutual interests □

Get to know more people □

Help others to keep in touch with me □

Find dates □

Find jobs □

Network in general □

Other □

Q5. On average, how often do you update your Facebook profile?

Several times a day □

Once a day □

Several times a week □

Once a week □

Several times a month □

Once a month □

A couple of times a year □

Never □

Q6a. Approximately, how many Facebook friends do you have?

____

Q6b. How many of these would you consider close friends?

____

Q6c. How many of these would you consider acquaintances?

____

Q6d. How many of these would you consider distant friends?

____

Q6e. How many of these have you met only on Facebook?

____

Q7. What are the specific ways you communicate with your friends using Facebook. Do you ever?

Check all that apply

Post messages to a friend's wall	□
Send a group message to all your friends	□
Send private messages to a friend within Facebook	□
Wink, poke, give "e-props" or kudos to your friends	□

Q8. What are the different reasons why you use Facebook?
(1 = strongly disagree, 2 = disagree, 3 = neither disagree nor agree, 4 = agree, and 5 = strongly agree)

I use Facebook ...	Strongly Disagree				Strongly Agree
To thank people	1	2	3	4	5
To let people know I care about them	1	2	3	4	5
To show others encouragement	1	2	3	4	5
To help others	1	2	3	4	5
To show others that I am concerned about them	1	2	3	4	5
To kill time	1	2	3	4	5
Because it is entertaining	1	2	3	4	5
Because I enjoy it	1	2	3	4	5
Because it is fun	1	2	3	4	5
Because it is a pleasant rest	1	2	3	4	5
Because it relaxes me	1	2	3	4	5
Because it makes me feel less tense	1	2	3	4	5
To get away from pressures and responsibilities	1	2	3	4	5
To not look old-fashioned	1	2	3	4	5
To look stylish	1	2	3	4	5
To look fashionable	1	2	3	4	5
To feel involved with what's going on with other people	1	2	3	4	5
Because I need someone to talk to or be with	1	2	3	4	5
Because I just need to talk about my problems sometimes	1	2	3	4	5
To make friends of the opposite sex	1	2	3	4	5
To be less inhibited chatting with strangers	1	2	3	4	5
To meet new people (new acquaintances)	1	2	3	4	5
To flirt with someone	1	2	3	4	5
To make plans with my friends	1	2	3	4	5
To get away from what I am doing	1	2	3	4	5
To put off something I should be doing	1	2	3	4	5

To forget about my problems	1	2	3	4	5
To feel connected	1	2	3	4	5
To feel less lonely	1	2	3	4	5
To do something with others	1	2	3	4	5

PART B:

The following two questions address general, non-Facebook related topics:

Q9. Think of a close friend who is **male** and a close friend who is **female**. Indicate **for both columns** below the extent to which you have disclosed to each person. **This includes both online and offline interaction.**

(From 1, which means you haven't discussed the topic at all, to 5 which means that you have discussed this topic fully and completely)

Disclosure Type	Male Friend					Female Friend				
My personal habits	1	2	3	4	5	1	2	3	4	5
Things I have done which I feel guilty about	1	2	3	4	5	1	2	3	4	5
Things I wouldn't do in public	1	2	3	4	5	1	2	3	4	5
My deepest feelings	1	2	3	4	5	1	2	3	4	5
What I like and dislike about myself	1	2	3	4	5	1	2	3	4	5
What is important to me in life	1	2	3	4	5	1	2	3	4	5
What makes me the person I am	1	2	3	4	5	1	2	3	4	5
My worst fear	1	2	3	4	5	1	2	3	4	5
Things I have done which I am proud of	1	2	3	4	5	1	2	3	4	5
My closest relationships with other people	1	2	3	4	5	1	2	3	4	5

Q10. How concerned are you, if at all, about Internet privacy?

Very concerned □

Somewhat concerned □

Not too concerned □

Not concerned at all □

Don't know/Refused □

If you do not use Facebook, please skip to question 12

Q11. We'd like to know if the following kinds of information are posted to your Facebook profile

Information Type	**Yes**	**No**	**Don't know/Refused Question**
Your first name	□	□	□
Your last name	□	□	□
Your school name	□	□	□
Your IM screen name	□	□	□
Your blog or link to your blog	□	□	□
Your e-mail address	□	□	□
Your cell phone number	□	□	□
Your current address	□	□	□
A photo of yourself	□	□	□
Photos of your friends	□	□	□
Your birthday	□	□	□
The city or town in which you live	□	□	□
Videos	□	□	□
Your political views	□	□	□
Your sexual orientation	□	□	□
Your relationship status	□	□	□
Your interests (books, movies, activities, Etc.)	□	□	□

Other ____

Q12. To what extent do you agree with the following statements…?

(1 = strongly disagree, 2 = disagree, 3 = neither disagree or agree, 4 = agree, and 5 = strongly agree)

	Strongly Disagree				Strongly Agree
Future employers will use the personal information contained on my Facebook site to assess my suitability for employment with their company	1	2	3	4	5
University admissions officers have started using the personal information on Facebook sites to assess applicant suitability prior to offering admissions	1	2	3	4	5
Police officers are using Facebook to track underage drinking and other illegal activities.	1	2	3	4	5
Universities are monitoring Facebook postings, personal information and images to identify university code violators (i.e. involvement in illegal activities)	1	2	3	4	5
Media accounts of the privacy risks (cyber stalking, surveillance, identity theft, etc.) associated with the disclosure of personal information on Facebook are inaccurate or untrue	1	2	3	4	5
Employers are using Facebook to monitor the extra-curricular activities of their employees	1	2	3	4	5
Sexual predators use social network sites such as Facebook to track, monitor and locate potential victims	1	2	3	4	5
Political parties have begun using Facebook to target young professionals and students through the use of advertisements and data mining	1	2	3	4	5

PART C:

If you do not use Facebook, please skip to question 17

Q13. Who is your profile currently visible to? If you are unsure, please select "Don't know/Refused"

Visible to anyone searching Facebook	□
Visible to all my networks and all my friends	□
Visible to some of my networks and all of my friends	□
Visible only to my friends	□
Don't know/Refused	□

Q14. We'd like to know what privacy settings (if any) you have activated. Have you made your information visible to…?

Information Type	**All my networks and all my friends**	**Some of my networks and all of my friends**	**Only my friends**	**Only me**	**Don't know/Refused Question**
Photos tagged of you	□	□	□	□	□
Videos tagged of you	□	□	□	□	□
Status updates	□	□	□	□	□
Online status	□	□	□	□	□
Friends	□	□	□	□	□
Wall	□	□	□	□	□
Courses	□	□	□	□	□
News Feed/Mini Feed	□	□	□	□	□

Q15. To what extent do you agree with the following statements…?

(1 = strongly disagree, 2 = disagree, 3 = neither disagree nor agree, 4 = agree, and 5 = strongly agree)

	Strongly Disagree				Strongly Agree
I have provided **FAKE** or **INACCURATE** information on Facebook to restrict people I don't know from gaining information about myself	1	2	3	4	5
I have **EXCLUDED** personal information on Facebook to restrict people I don't know from gaining information about myself	1	2	3	4	5
I have sent private email messages within Facebook instead of posting messages to a friend's wall in order to restrict others from reading the message	1	2	3	4	5
I have **BLOCKED** former contacts from contacting me and accessing my Facebook profile	1	2	3	4	5
Certain contacts on my Facebook site only have access to my limited profile	1	2	3	4	5
I have changed the default privacy settings activated by Facebook	1	2	3	4	5
I have deleted messages posted to my Facebook wall to restrict others from viewing/reading the message	1	2	3	4	5
I have untagged myself from images and/or videos posted by my contacts	1	2	3	4	5

Q16. Thinking about the **LAST** time you were contacted on Facebook by someone who was a complete stranger to you, how did you respond?

Just ignored the request for authorization or deleted the request for authorization	□
Accepted the request for authorization so I could find out more information about the person	□
Accepted the request for authorization and told them to leave me alone	□
Reported the person to Facebook staff	□
Blocked the person from contacting me	□
Other	□

PART D:

Q17. How old are you? ____________________

Q18. What is your sex?

Male □

Female □

Refused Question □

PART E:

Your participation in this study qualifies you for a chance to win one of four Tim Hortons' gift certificates valued at $10 each.

Would you like to be entered into the draw for a chance to win one of the Tim Hortons' gift certificates?

Yes □ No □

If yes, please provide your contact information (Name and email address)

____

PLEASE DETACH THIS PAGE, FOLD AND PLACE IN THE DRAW BOX LOCATED AT THE FRONT OF THE CLASSROOM.

Appendix E. Interview Guide

A. DEMOGRAPHICS

1. Age ______
2. Sex _______
3. Year of enrollment _____________
4. Program/Faculty _________________

B. ADOPTION AND USE OF FACEBOOK

1. When did you first start using Facebook? _________________

   Year and grade/program level
2. Who, if anyone, introduced you to it? ___________________

   Self, friend, family member, etc.
3. What was you primary motivation for joining? _____________
4. What do you primarily use Facebook for? _________________

   Converse with friends, check up on the activities of friends, make new friends, etc.
5. On average, how often do you log into your Facebook account? For how long? Is there any variation in use? Weekends, Weekdays, AM, PM.
6. Approximately, how many friends do you have listed to your Facebook profile?
7. Of these friends, how many would you consider to be:
   a. Close friends
   b. Acquaintance
   c. Family
   d. People you've only met on Facebook
8. What is your primary means of communication in Facebook?

   Wall, group email, private email, poke

C. CONCERN FOR PRIVACY

1. Are you concerned about privacy on the Internet?
   a. If yes, why? What are you concerned about?
      Surveillance, cyber-stalking, harassment, etc.
   b. Have you had any negative experiences? Tell me about it

c. Have you developed any tactics to protect yourself against privacy threats while using the Internet?
Self-censorship, fake or inaccurate information, exclusion of information. etc.

d. If no, why are you not concerned?

2. Are you concerned about privacy in Facebook?

D. SELF-DISCLOSURE ON FACEBOOK

1. Have you provided the following information on your profile page?

Your full name □

Your first name □

Your middle name □

Your last name □

Other □

Your birthday □

Day □

Month □

Year □

Other □

Your sex □

Male □

Female □

Other □

Your phone number □

Cell number □

Landline number □

Other □

2. Have you purposely **Excluded** information from your profile?
   a. If yes, what information have you excluded? ____________________
   b. Why have you excluded this information?
   c. If no, why have you chosen not to exclude any information?
3. Is your profile image an accurate self-depiction? _______________
   a. If yes, what was your reason for posting an accurate self-image?
   b. If no, what was your reason for posting an inaccurate self-image?

Humour, joke, concealment, etc.

4. Is any of the information included in your profile **Fake** or **Inaccurate**?

 ____

   a. If yes, what information is fake or inaccurate?
   b. Why have you provided fake or inaccurate information?

5. Have you ever **included** information on Facebook that you now regret providing?

 ______

   a. If yes, what information do you regret including? ___________________
   b. Why do you regret including this information? i.e. was the information used to harm you?
   c. Have you since removed the information from your profile? ____________
   d. If no, explain why not

6. What influences your decision to either disclose or conceal information on Facebook? In other words, when deciding what personal information to include or withhold, what factors influence your decision?

E. USE OF THE PRIVACY SETTINGS

1. Who has access to your profile? ________________

 Anyone, all of your networks and all of your friends, some of your networks and all of your friends, only your friends

   - If anyone mentioned, ask why they feel comfortable allowing anyone on Facebook to access their profile

2. Have you blocked anyone from access to your profile? ______________
   a. If yes, who have you blocked? ____________

    Stranger, friend, acquaintance, family member, etc.

   b. Why have you blocked this person?

3. Have you ever reported someone to Facebook staff? _________
   a. If yes, why did you report this person?

    Fake profile, harassment, inappropriate content, etc.

4. You can find you using the search function? _______________

Anyone, all of your networks and all of your friends, some of your networks and all of your friends, all of your friends

a. What can people do with your search results?

View your profile page □

Send you a message □

Poke you □

Add you as a friend □

View your list of friends □

5. Are you aware that, unless otherwise specified, people can search for your Facebook profile in Google?
    a. If yes or no, how does this make you feel? Do you think this is an invasion of your privacy? Or do you think this is a beneficial feature? Why or why not?

F. WILLINGNESS TO 'FRIEND' STRANGERS

1. Have you ever accepted a friendship request from a stranger? _______
    a. If yes, why?

       To make a new friend, to find out more information about the person, to increase your list of contacts, to create an illusion of popularity, etc.

        i. Is the person still on your contact list? _________
        ii. If yes, have you engaged in conversation with them? _____________
        iii. If no, why not? Did something happen that made you decide to remove them?
    b. If no, explain why not
        i. What action(s) did you take?

           Ignore, block, report, etc.
2. How do you decide whether or not to 'friend' someone?
    - Make sure to inform respondent that this question includes all friendship requests from friends, acquaintances, family members, strangers, etc.

Appendix F. Thematic Framework

1. **Facebook Adoption and Use**
    - 1.1. Adoption Date (year and grade/program level)
    - 1.2. Introduction to Facebook
    - 1.3. Reason(s) for Joining Facebook
    - 1.4. Reason(s) for Using Facebook
    - 1.5. Frequency and Length of Facebook Visits
    - 1.6. Network Size and Breakdown by Relationship Type
    - 1.7. Communication Practices in Facebook
2. **Privacy Concerns**
    - 2.1. Internet Privacy Concerns
        - 2.1.1. Type(s) of Concern
        - 2.1.2. Negative Experiences
        - 2.1.3. Protection Techniques
    - 2.2. Facebook Privacy Concerns
        - 2.2.1. Type(s) of Concern
        - 2.2.2. Negative Experiences
        - 2.2.3. Protection Techniques
3. **Information Revelation on Facebook**
    - 3.1. Information Posted to Facebook Profile
    - 3.2. Information Excluded from Facebook Profile
    - 3.3. Factors Influencing Information Revelation on Facebook
4. **Privacy Protection**
    - 4.1. Profile Visibility
    - 4.2. Search
    - 4.3. Limited Profile
    - 4.4. Blocked
    - 4.5. Use of Fake or Inaccurate Information
5. **Friending on Facebook**
    - 5.1. Factors Influencing 'Friending' on Facebook

Appendix G. Thematic Framework Matrix (Example)

INFORMATION REVELATION	3.1	3.2	3.3
Pseudonym, Age, Field of Study	**Information posted to profile**	**Information excluded from profile**	**Factors influencing information revelation**
Michael, 32, Humanities	Full name Sex Profile image	Cell phone/landline number Birth date	(1) "The less people know the better" (2) Profile image - "I have nothing to hide – especially since the friends I am contacting are high school friends – it's reciprocal; they post their pictures of themselves" (easier for friends to find in search) (3) Disclosure in general - "If they want to know about me, they'll send a message. I don't want the person to just read about me, I want them to ask me."
Christine, 18, Business	Full name Birth date (no year) Sex Profile image	Cell phone/landline number "I don't have much written in any of my fields. I mean, I think I have one favourite movie and a quote … I personally don't disclose much on it other than the basic, like your name and your sex"	(1) Disclosure in general -"If someone wants to know about me, they can ask me. It kind of annoys me when you're scrolling down and there are pages and pages of information and a lot of the time it's really irrelevant to me. So, I personally don't post it" (2) Profile image - "Well, the people that will be viewing my profile are my friends." A picture of self connects the profile. "It's your page so there obviously should be a picture of you – that's the way I see it." (3) Factors - Three things: (1) is it something that I would want a younger person who possibly looks up to me to see it?; (2) is it something I wouldn't mind my parents seeing?; and, (3) is it something that I want employers to look at? – Is it something that would be acceptable in other people's eyes?

Appendix H. Guidelines

Privacy Issues and Controls in Social Network Sites

Social network sites or SNSs are virtual spaces on the Internet where users can create a profile and link that profile to friends for the purpose of creating a personal network. Social network site profiles typically contain information about the user, including their real name, email address, education information and interests, and are created with the intention of finding or being found by others. Some of the most well known social network sites include Facebook, MySpace and Friendster. Students at the University of Western Ontario primarily use Facebook.

Privacy Issues

1) **Data Mining**: Facebook's terms of use agreement indicates that they reserve the right to use or appropriate any information disclosed on the site for a multitude of purposes, such as advertising. Even if users have restricted their profile only to friends, that is to their personal networks, any information they provide on Facebook (this includes pictures, writings on walls, fun messages, etc.) can be used in the media or by third parties without authorization of the user. This poses serious privacy risks and users should be aware of the potential unwanted use of their data and the social consequences this use can have on their lives.

2) **Archival of Data:** Information provided on social network sites can be easily downloaded, archived and searched. Users' information may not be used by third parties at the present time, but could be used in the future without requiring the permission of the user. Hence, individual's behaviors can leave a trace in virtual space.

3) **Current or Future Employers**: Employers can use social network sites to monitor the activities of their employees and to assess the suitability of applicants. Restricting access of one's profile visibility to friends (see point 1 under Privacy Controls) is a good strategy to protect oneself from unwanted audiences, such as current or future employers. However, it is important to realize that privacy breaches have occurred on social network sites in the past, where outsiders have hacked into profiles or where someone who is a member of the users' network has extracted information. While information is relatively well protected, one has to be aware of the fact that there can be leaks. Therefore, content on social network sties should not be considered 100% secure.

4) **Universities**: Users also need to be aware of the fact that if violations of university conduct take place within social network sites this could potentially affects students' status within the university. At York University there was a recent case where a student employed Facebook to create a study group and later faced expulsion being accused of having used the site for exchanging solutions to assignments, which is considered cheating.

5) **Surveillance, Identity Theft, & Stalking**: The disclosure of personally-identifiable information such as physical address, phone number(s), residence information, class schedules, etc. increases users' chances of being followed offline. This can place individuals at a greater risk for surveillance and stalking. Identity theft is also a concern and therefore little personal information should be included on social network sites.

Privacy Controls

1) **Profile visibility**: Users can control who has access to their profile by changing the visibility of their profile. Most SNSs have features that allow users to control their privacy. For example, Facebook offers four levels of profile visibility: 1) "*all networks and all friends*", which enables all individuals in the same networks as the user (i.e., UWO and London) and all the user's friends to view the user's profile, 2) "*some networks and all friends*", which enables individuals in specified networks and all the user's friends to view the user's profile, 3) "*friends-of-friends*", which enables friends of the user's friends to view the user's profile, and 4) "*friends only*", which restricts access to the user's immediate group of friends on Facebook.

2) **Information visibility**: As of March 2008, Facebook added additional privacy controls, which afford users more control over the information they chose to post to their profiles. Users can now restrict certain individuals or groups of individuals from seeing their basic information, personal information, status updates, photos tagged of the user, wall, list of friends, education information, work information, etc. This provides greater flexibility to display identity while protecting key personal information.

3) **Exclusion of information**: Another option for users is the exclusion of information. Aside from name, email address and birth date, the remainder of the profile fields are optional and are not required to join Facebook. Another strategy employed by users to evade identity theft is to provide somewhat altered information.

Best Practices

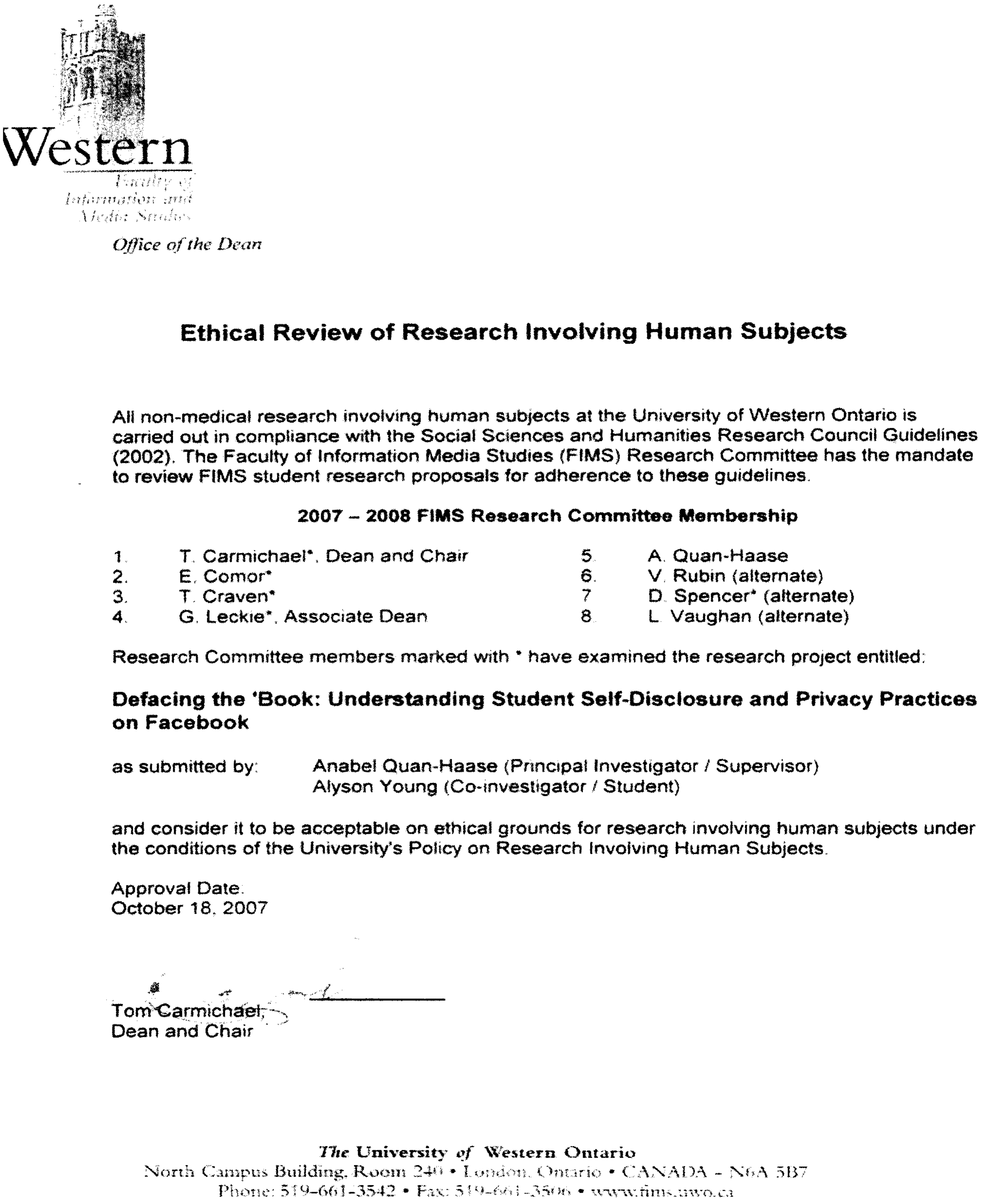
For users to protect themselves against the various privacy risks associated with the use of social network sites, such as Facebook, the ideal solution is to employ a combination of the privacy controls described above.

- Adjusting the user's profile visibility to *'only friends'* reduces the likelihood of unwanted audiences accessing one's profile and viewing the information contained within.

- The exclusion of certain types of information further ensures that in the event that unwanted audiences gain access to one's profile, highly private or personal information, such as addresses, phone number(s), SIN number, etc., is not accessible and cannot be used in ways to harm the user.

- Privacy is further protected by not including information about whereabouts, others' telephone numbers or other personal information on the profile, the fun wall or other applications within Facebook.
- Users can further optimize their privacy by employing the information visibility control options available to restrict visibility by relationship status, e.g., acquaintances, work associates, and family members, from accessing certain types of information.

Appendix I. Ethics Approval



Western
Faculty of
Information and
Media Studies

Office of the Dean

Ethical Review of Research Involving Human Subjects

All non-medical research involving human subjects at the University of Western Ontario is carried out in compliance with the Social Sciences and Humanities Research Council Guidelines (2002). The Faculty of Information Media Studies (FIMS) Research Committee has the mandate to review FIMS student research proposals for adherence to these guidelines.

2007 – 2008 FIMS Research Committee Membership

1. T. Carmichael*, Dean and Chair
2. E. Comor*
3. T. Craven*
4. G. Leckie*, Associate Dean
5. A. Quan-Haase
6. V. Rubin (alternate)
7. D. Spencer* (alternate)
8. L. Vaughan (alternate)

Research Committee members marked with * have examined the research project entitled:

Defacing the 'Book: Understanding Student Self-Disclosure and Privacy Practices on Facebook

as submitted by: Anabel Quan-Haase (Principal Investigator / Supervisor)
Alyson Young (Co-investigator / Student)

and consider it to be acceptable on ethical grounds for research involving human subjects under the conditions of the University's Policy on Research Involving Human Subjects.

Approval Date:
October 18, 2007

Tom Carmichael,
Dean and Chair

The **University** *of* **Western Ontario**
North Campus Building, Room 240 • London, Ontario • CANADA – N6A 5B7
Phone: 519-661-3542 • Fax: 519-661-3506 • www.fims.uwo.ca