2011

To Tell or Not to Tell: Predictors of Disclosure and Privacy Settings Usage in an Online Social Networking Site (Facebook)

Amanda Nosko
Wilfrid Laurier University

Your file Votre référence
ISBN: 978-0-494-75404-7
Our file Notre référence
ISBN: 978-0-494-75404-7

To Tell or Not to Tell: Predictors of Disclosure and Privacy Settings Usage in an Online Social Networking Site (Facebook).

by

Amanda Nosko

M.A. Wilfrid Laurier University, 2006

B.A. University of Waterloo, 2004

DISSERTATION

Submitted to the Department of Psychology/Faculty of Science

in partial fulfillment of the requirements for

Doctor of Philosophy in Psychology

Wilfrid Laurier University

Abstract

Use of social networking sites has grown exponentially over the last decade. Facebook, a popular social networking site, currently boasts membership of over 500 million users (www.facebook.com). In the present research, four studies were conducted to examine factors that impact on self-disclosure and privacy settings use. The primary goal for Studies 1A, B and C involved developing methods for organizing and understanding the information that individuals disclose through social networking sites. Specifically, in Study 1 A, a scoring tool was developed in order to comprehensively assess the content of the personal profiles. In Study 1 B, grouping categories (default/standard information, sensitive personal information, and potentially stigmatizing information) were developed to examine information pertinent to identity threat, personal and group threat. Finally, in Study 1 C, an alternative grouping strategy was developed to include all information present in Facebook, organized as a function of the content that was presented. Overall, these studies indicated that approximately 25% of all possible information that could potentially be disclosed by users was disclosed. Presenting personal information such as gender and age was related to disclosure of other sensitive and highly personal information as well as greater disclosure. As age increased, the amount of personal information in profiles decreased. Those seeking a relationship were at greater risk of threat, and disclosed the greatest amount of highly sensitive and potentially stigmatizing information. Study 2 examined whether giving participants stories to read that did or did not alert participants to potential dangers of disclosure and the media context (electronic or hard copy formats) impacted on disclosure and privacy

settings use. In addition, the predictive power of gender and the virtual other (the audience in mind) was also examined. Females disclosed less sensitive information than males after reading a personal privacy invasion story. Disclosure was less when the target for whom the information was being posted was the same gender as the participant, and more when the target was the opposite gender of the participant. Disclosure of specific content areas also differed by gender of the discloser. Only 20.3% of participants employed privacy settings. When a virtual audience consisting of referents other than friends or the self was in mind, use of privacy settings increased. Lastly, participants who filled out Facebook profiles on paper-and-pencil disclosed more as compared to their online Facebook counterparts. Overall, these findings shed light on some of the factors that may be related to over-disclosure, and help to identify those users who are at particular risk when online. In addition, these studies examined a relatively novel but highly important area, privacy settings and the factors that relate to use. The notion of the virtual other is one that demands further examination and may prove useful in understanding how and why people choose to share highly personal information online, and most importantly, employ privacy settings.

Acknowledgments

I would first like to thank the best advisor anyone could hope for, Dr. Eileen Wood. As William Ward once said, "The mediocre teacher tells. The good teacher explains. The superior teacher demonstrates. The great teacher inspires." Not only has Eileen been an inspiration intellectually, but she has continually offered unconditional support and guidance, and has taught me what it means to be a true mentor. Because of Eileen, the experiences over the past 6 years have been the most important and formative in my life. I came to Laurier with an interest in Psychological research, and I leave with a lifelong love for it.

The members of my dissertation committee, Dr. Alexandra Gottardo, Dr. Christian Jordan, Dr. Lisa Wood and Dr. Robert Orr have generously given their time and expertise to better my work. Thanks to all of you for your wonderful insight.

I would also like to thank the fantastic lab mates I have been lucky enough to have other the last few years. Domenica, Lucia, Karin, and Seija, thanks for your support and company, especially near the end when I never thought I'd finish! Thanks to great friends Vanessa, Amy, Alana and Thanh, you guys were my rocks throughout graduate school.

I would like to thank my wonderful family. Thanks to mom and dad for always being supportive and understanding of my perpetual student-hood and for teaching me to keep a positive attitude no matter how hard things get. Finally, to my best friend and husband Robin. Words can't describe how much I appreciate having you in my life.

Table of Contents

List of Tables

List of Figures

To tell or not to tell: Predictors of Disclosure and Privacy Settings Usage in an Online Social Networking Site (Facebook).

"I like Facebook because I can post things about myself, and also see what other people have posted" (female, 23)

Throughout history, technological advancements have changed the nature of social communication. Before the age of the telephone, people corresponded either face-to-face, or through written letters. With the advent of the telephone, people were able to communicate across long distances, and could exchange verbal messages virtually instantly. Over the last few decades, with the advent of the Internet, social communication has gone through yet another transformation. Email, instant messaging (IM, MSN) and online profile sites have become a quick and easy mode for communicating with close friends and strangers alike. The Canadian Internet Survey conducted in 2009 asked 23,000 Canadians about their Internet use. Results reported that 21.7 million Canadian households (80%) were connected to the Internet and reported using it for personal reasons. When frequency of Internet use per day was examined, results revealed that 3/4 of the population used the Internet every day. Eighty-one percent of men and 80% of women used the Internet in 2009. When asked about specific use of the Internet, approximately 7 out of every 10 users resorted to using the Internet for information seeking (e.g., reading the news, searching for health information) and online banking. The top reason for going online in 2009 was for social communication purposes, specifically for accessing email (91%). Interestingly, those who had been using the

Internet for more than five years were less likely to be concerned about online security. As the popularity of the Internet continues to grow, researchers may expect to see a continued increase in the frequency of online social interaction. Even more, as popularity with online media increase, it is possible that the ease with which users can communicate coupled with a growing familiarity with technology may contribute to drastic reductions in the use of more traditional forms of communication, including the telephone and written letters. How people are using this technology, and how the online social context differs from offline interaction warrants investigation. The concomitant arrival of wireless technology has made the possibility of online communication even more prevalent by increasing the opportunity for connection (Internet World Stats: Usage and Population Statistics, 2010). Wireless connection to the Internet can be attained remotely (from any location) that provides a wireless router. Plugging in a cord to access the Internet is no longer required to connect.

It has been proposed that the Internet operates as a powerful 'Triple A Engine', consisting of *accessibility* (anytime, anywhere), *affordability* (most sites allow for free use), and *anonymity* (the ability to protect one's identity) (Cooper, Shapiro & Powers, 1998). This combination of factors makes the Internet a very appealing outlet for social communication. Given the prevalence of computer technology in society and the opportunities it affords for social interaction, it is important to understand the unique role that computers may have in social communication. The present research is a first step to understanding the role computer technology, and more specifically online social networking plays in social interaction. More specifically, the present research examines

variables that might impact on disclosure online as well as use of privacy settings in social networking profiles.

What are Social Networking Sites?

Social networking sites (SNSs) (e.g., Facebook) are web-based social communication tools designed to allow users to contact and communicate with other users. The three key features that define SNSs according to Boyd and Ellison (2007) are that the sites "allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system" (pg. 2). Personal web-pages and online profile networks have emerged at an increasing rate on SNSs and continue to gain popularity (Yum, 2007).

Why Do People Use Social Networking Sites?

Researchers have started to examine how and why people are drawn to SNSs and social media platforms. Research examining Facebook, for example, has identified multiple reasons that explain why users establish and maintain personal profiles including: interconnection and the desire to bridge offline and online relationships (Boyd & Ellison, 2007), maintenance of existing offline friendships (Ellison, Steinfield, & Lampe, 2007; Lenhart & Madden, 2007; Madge, Meeks, Wellens, & Hooley, 2009; Wiley & Sisson, 2006), identity formation (Selwyn, 2009; Stutzman, 2006; Valkenburg, Schouten, & Peter, 2005) self-expression and self-disclosure (Wiley & Sisson, 2006), and "lurking" or browsing information of other users (Pempek, Yermolayeva, & Calvert,

2009). Additionally, SNSs allow users to express themselves openly and freely, and in fact, encourage just that.

Although SNSs may represent potentially new learning tools, their introduction requires careful consideration in order to avoid pitfalls that could lead to vulnerabilities for the user. Access, information, building relationships and sharing with others are the hallmarks of social network sites. By simply typing in a person's name, an abundance of information can be accessed, ranging from relatively benign pieces of personal details such as favorite quotes, to highly personal pieces of information including profile pictures, home addresses and birth dates.

Users may not consider the implications of their disclosures online, and may not realize that they can put themselves and others at risk either directly or indirectly by sharing information in an open forum. The very openness, connectedness and accessibility offered through SNSs have the potential to place users at risk, but the sites also have mechanisms to minimize risks. The following sections will describe a popular SNS (Facebook) and identify the pitfalls associated with use of SNSs.

What is "Facebook"?

Facebook, founded in 2004, was originally designed as a SNS for students at Harvard University. Its popularity has grown immensely and expanded beyond the initial Harvard setting with the potential to include anyone anywhere in the world who is older than 13 years of age. Facebook currently has over 500 million active users and as such is the leading social network site in the world. The infrastructure of Facebook is comprised of a variety of networks. Each network represents a company, school (e.g.,

university/college) or geographical region (e.g., city, state, or province). Individuals create a profile within one network. Creation of an account is necessary for membership and requires that the user provide basic information including a valid email address, as well as identify a gender, and provide a birth date. Once a member, users can create a personal profile for themselves which may include information such as their age, gender, personal preferences, and location. They can also upload pictures, describe interests, education, relationships, and more. Facebook offers users the opportunity to search for friends by typing their names into the search bar (these can be actual friends, acquaintances or even strangers), and add them to their "friends list". Users can interact with one another either through a personal message, similar to an email inbox, or by posting more public messages on the profile wall, a feature similar to a bulletin board. Another attractive feature of Facebook is the capacity to create and join groups that may be based on similar interests, mutual causes, or are simply for fun. For a complete glossary of Facebook terms, refer to Appendix A.

What are the Associated Risks with SNSs?

When users initially sign up for a Facebook account, they are required to provide at least a few personal details (e.g., date of joining, birth date, email address and name). Once a member, many users go beyond just the bare minimum and provide a wide variety of personal information in their profiles (e.g., location, mobile phone number, sexual orientation, personal photos). The default setting for a new profile allows public access to any other user within the new user's specified network. As well, the new user's profile is accessible to the friends of all the other users within their network. Given that users are

providing sensitive information online, they may place themselves at considerable risk. For example, Facebook users may subject themselves to potential embarrassment, identity theft, "lurking" or stalking by other users, and blackmailing (Gross & Acquisti, 2005).

Just How Serious Can Over-Disclosure of Personal Details Be?

In some cases, Facebook users have posted directions to personal residences and cottages along with wall updates notifying others that they are out of town for the weekend - providing an open invitation to thieves to come over to an empty, unsupervised house. During a two month-long investigation that tracked more than a dozen Canadians through their open social-networking profiles, a reporter for a national newspaper, "The Globe and Mail", built profiles for individual users (Hartley, 2008). Here are examples of some of the information extracted about individual users:

> "A 24-year-old Calgary woman posts her cell phone number, e-mail address, and the name of the Kelowna motel where she and three of her friends will spend a June weekend partying. In addition to nicknaming the event the "Erotic Party," the women joke about finding "some hot men to buy us dinner and drinks."
>
> "A Toronto teen posts comments about her favourite sexual positions; a 24-year-old Saskatchewan man posts details for a huge house party he plans to hold while his parents are out of town."

The reporter went on to explain that while some of these stand alone details may not amount to much, through use of freely available web tools including directory searches (e.g., Canada411) and Google (e.g., using the reverse phone search on

Canada411), other users could easily look up related personal information, including home addresses and directions to personal residences. In one instance, the reporter even went so far as to meet up with a 17 year old female, whose profile he found on Facebook. The teenager's cell phone number was posted on her open Facebook profile, and this is how he contacted her. After agreeing to meet, he showed her the profile he had constructed for her based on information she had posted, including, but not limited to, where she lived, where she worked, her home and cell phone numbers, and her birth date.

Defining Self-Disclosure

Self-disclosure generally refers to any message conveyed about the individual, and can be subdivided into various types. First, there are two broad categories of self-disclosure that describe the statements made by an individual in terms of descriptive or affective content. Self-disclosure that consists of general facts about a person, such as "My favorite colour is blue", or "My family comes from Germany" is called *descriptive self-disclosure* (Derlega, Metts, Petronio & Margulis, 1993). Messages that convey expressions about feelings and opinions are called *evaluative self-disclosures* and include statements such as "I hate writing exams", or "I feel angry that you said that to me". Aside from the two broad categories of self-disclosure, it is also useful to distinguish the type self-disclosure based on the referent, that is, whether the disclosure involves divulging information about one's relationships and interactions with others (*relational* self-disclosure) or information about oneself (*personal* self-disclosure).

Relational self-disclosure has been the main focus of self-disclosure research (e.g., Levesque, Steciuk & Ledley, 2002). This form of self-disclosure has been deemed

particularly salient in close relationships as it may have a very beneficial role in relationship maintenance. For example, when romantic couples are able to talk to one another about the status of a relationship it may help the couple deal with conflict (Waring, 1987). In comparison to research examining relational self-disclosure, no known studies have looked at self-disclosure online from a personal standpoint where disclosure occurs without the expectation of interaction. The relative lack of literature exploring personal self-disclosure calls for examination of this less researched form of communication.

The act of self-disclosing is a key component of close relationship formation and maintenance (Altman & Taylor, 1973). Many things can affect what information is disclosed and for whom it is disclosed. Both theory and research on self-disclosure have attempted to identify variables which impact on what is disclosed, how much is disclosed, and who is the recipient of disclosure, including: gender differences (e.g., Derlega & Chaikin, 1976; Dindia & Allen, 1992), and trust (Wheeless, 1978; Wheeless & Grotz, 1977).

Gender Differences in Self-Disclosure

A large body of research has examined how males and females differ in terms of self-disclosure. Effect sizes from a meta-analysis of gender differences in self-disclosure conducted by Dindia and Allen (1992) revealed that, in general, females disclosed more information about themselves than did males. In addition, when compared to their male counterparts, females disclosed more to strangers. Moreover, same-sex and opposite sex dyadic interactions showed that female-female disclosure was the highest and male-male

disclosure was the lowest, with male-female disclosure in the middle. In line with reciprocity theory, it was speculated that these results occurred because of more female and less male disclosure overall, thus canceling out the polar effects, and resulting in moderate disclosure. That is, while females disclose more, and males disclose less, partners either encouraged or discouraged disclosure, resulting in the observed moderate level of overall disclosure.

Early psychologists attributed these gender differences in self-disclosure to sex roles, such that males were expected to be emotionally unexpressive and females were taught to be emotionally expressive (Derlega & Chaikin, 1976), thus encouraging differential levels of disclosure as a function of gender. In the case of self-disclosure, it would not be appropriate or acceptable for a man to disclose intimate details about the self, without fear of rejection or social disapproval from peers and/or strangers. Researchers even went so far as to imply that men who exhibited higher levels of self-disclosure were less psychologically stable (Derlega & Chaikin, 1976) due to the conflict between gender role expectations and behaviours.

Perhaps males may not be as expressive emotionally as females in everyday conversation, but they may still be inclined to disclose. It is possible that this disclosure may be content-dependent. Men may be comfortable talking about topics related to popular activities and less feminine activities such as sports or even on more taboo topics including sexuality. For example, men felt more positive about sexual material, and were also more likely to seek out this material (Nosko, Wood, & Desmarais, 2007). It is

proposed that disclosure by males may be topic dependent (Derlega, Durham, Gockel & Sholis, 1981), especially in settings where there are fewer social pressures (e.g., online).

Disclosure and Trust

Trust plays an important role in self-disclosure. Early work examined and conceptualized trust in several ways including situations that require trust in order to achieve mutual goals (e.g., Giffin, 1967); risky behaviours which indicate trust (e.g., Pearce, 1974); and positive perceptions of those who are trustworthy (e.g., Giffin, 1967, Wheeless & Grotz, 1977). Revealing personal information can be seen as a risky behaviour in many situations. When personal information is offered to someone, the threat of exposure or unwanted revelation of intimate details to a public audience is ever-present. In order for people to feel comfortable disclosing, they need to feel as though they can trust the receiver of their disclosure. Self-disclosure, therefore, may be a behavioural indicator of trust, whereby the more trustworthy someone is perceived to be, the greater the likelihood of that person receiving intimate disclosures. This same phenomenon may occur online where, instead of a person being perceived as trustworthy, the system (i.e., the Internet) or a specific site is perceived as trustworthy, thus encouraging greater self-disclosure.

Impact of Vivid Stories

Aside from gender and trust, it is suggested that anecdotal stories may also play a role in disclosure. Various studies in the area of decision making have noted the powerful influence of anecdotal stories (de Wit, Das, &Vet, 2008; Fagerlin, Wang & Ubel, 2005; Hamill, Stanovich, 2009; Wilson, & Nisbett, 1980). Not only do vivid anecdotes engage

learners, but they increase meaning making (Bruner, 1996). While this can be seen as beneficial in certain cases, an affinity for stories can sometimes lead to the disregard of more reliable and accurate sources, including statistical and legal information (Stanovich, 2009). In the case of disclosure, it is suggested that the impact of a vivid anecdote about the potential consequences of disclosing personal details may encourage greater vigilance when disclosing. Moreover, because personal accounts are such powerfully persuasive tools, vivid anecdotal stories may also overshadow the impact of more formal legal documents, and may be more likely to impact on disclosure than formal privacy policies.

Self-Presentation (Impression Management)

Self-presentation is defined as a form of self-impression management and positive display of personal details (Goffman, 1959). Goffman (1959) originally developed a theory of self-presentation to explicate people's self-disclosure motives. Social life, according to Goffman's theory, is described as a multi-staged drama that highlights the actor-audience relationship. Strategic manipulation of presented information in this "drama" occurs in two ways, through information given (e.g., verbal communication) and information given off (e.g., non-verbal cues such as body language). The interaction between actor (presenter of information) and audience (the receiver of information) occurs based on the agreement that each person will accept the information revealed by the other, and will react accordingly to the information presented. Goffman posited that people assume their audiences will take seriously the self that is presented to them, and by extension, the impressions formed as a function of the presented information.

Goffman went on to identify various components of self-presentation. He asserted that the performance by an individual that is consistent and strong enough to influence the observers is called the 'front'. Moreover, the setting, or the items that are most commonly associated with a particular individual (e.g., gender, race, physical features, habits) are part of the overarching concept of the 'front'. The actor can manipulate how these features are displayed, and by extension, alter their performance to fit their audiences' expectations.

Self-presentation theory posits that social interaction is a dramatization and people are inclined to present themselves in an idealized way. What people choose to present to others may be dictated by their particular society, and often reflects or exemplifies the more desirable qualities of that particular culture. Goffman distinguished this idealized self, and called it our "social self". In comparison to our "flawed" or "realistic" self, in which we express genuine qualities (both positive and negative) and exhibit more variability in our behaviour, the "social self" tends to adhere more strictly to a set of consistent and desirable behavioural patterns. People present different variations of their "social self" depending on the social context and their interaction partners. In the case of online communication, where non-verbal cues are lacking, the opportunity to present an "idealized self" or the "social self" may be even greater (Cornwell & Lundgren, 2001; Walther, 1996). With fewer cues to base impressions on, there may be more room for misinterpretation, and for exploitation of desirable characteristics on the part of the user/actor. In the case of online profiles, users may take full advantage of the limited interactive aspect, and display highly idealized aspects of the self.

Self-Disclosure and Self-Presentation

Self-disclosure often occurs in tandem with self-presentation, and both processes are important in relationship development offline (Taylor & Altman, 1987). People have the desire to present themselves in a way that is seen as positive (Godfrey, Jones & Lord, 1986), and tend to display or convey their best qualities (e.g., best characteristics or most admirable accomplishments), while avoiding presenting aspects of the self that may be seen as less desirable, especially in the case of initial relationship development. Even when interacting with strangers, people engage in self-enhancement (Schlenker & Pontari, 2000). As choices are made about which self-relevant details to present, levels of self-disclosure are adjusted to match the guidelines of what is acceptable as set out by society or the situation. These processes are crucial during initial social encounters, because this information is used by interaction partners to determine whether or not to pursue and/or maintain the relationship (Derlega, Winstead, Wong, & Greenspan, 1987). While these two terms are related and important components of relationship formation, they are not interchangeable (Schlenker, 1986). Self-disclosure is primarily used to explain relationship formation, whereas self-presentation applies more generally to the strategic presentations of self-relevant details, in spite of a relationship context.

Theories of Self-Disclosure: Social Exchange & Social Penetration, Reciprocity, and Social Information Processing Theory

Several theories have been derived with the purpose of characterizing and clarifying the self-disclosure process. Specifically, four theories will be addressed in the following sections, including social exchange theory (Thibaut & Kelley, 1959), social

penetration theory (Altman & Taylor, 1973), the reciprocity norm (Gouldner, 1960), and social information processing (Walther, 1992).

Social Exchange Theory

Social exchange theory is based on the exchange of social and material resources, and lies at the heart of social interaction. Social exchange theory can be applied to self-disclosure by highlighting the reward/cost aspect of self-disclosing. Generally, relationships proceed from non-intimate to more intimate interactions (e.g., verbal and non-verbal communication and mutual activities) and are determined by the rewards and costs associated with past, present and future exchanges (Altman & Taylor, 1973). For example, when considering whether or not to develop a close relationship with another person, people may be inclined to assess what is being put into the relationship, and what is gained from being in the relationship. For the most part, people aim to maximize the benefits and minimize the costs associated with close relationships. When the benefits outweigh the costs associated with a particular relationship, then people may be more inclined to develop a close relationship and, by extension, may be more likely to disclose personal details. As people invest more into close relationships, disclosure increases and the relationship grows.

Social Penetration Theory

Similarly, social penetration theory (Altman & Taylor, 1973) focuses on reward/cost and how this affects the acquaintance process or "getting to know" process. This theory takes into account the joint effects of verbal as well as non-verbal interactions, and stipulates that there is a gradual, orderly process by which relationships

are formed. If this process is disrupted, relationships may suffer (e.g. too much disclosure initially may result in dislike). Social penetration theory consists of five stages that progressively increase in intimacy: *the orientation stage; the exploratory affective stage; the affective stage; the stable stage; and the depenetration stage*. In the first stage of this theory, the *orientation stage*, people are more cautious about the types of information they divulge. Typically, small talk occurs, whereby partners exchange trivial personal details, and generally adhere to socially acceptable disclosure. In the *exploratory affective stage,* people begin to express basic opinions (e.g., their political opinions) and continue to disclose increasingly more personal details. At this stage, interaction partners are still concerned with acting in socially desirable ways, and are not fully comfortable exposing themselves completely to their partner. This stage generally encompasses casual relationships. In the *affective stage*, more intimate details are discussed. People may disclose personal information to their partner, and discussions and disagreements may arise. In the *stable stage*, partners are able to fully disclose intimate personal information, and can often predict how their partner will react to the information received. At this point, the social relationship plateaus. In the last stage of the theory, or the *depenetration stage*, relationship dissolution may or may not occur. The costs begin to outweigh the benefits associated with the relationship, and partners are faced with the choice of whether or not to terminate the relationship.

The Reciprocity Norm

In addition to social exchange and social penetration theory, norms outlining expected behaviour impact on personal information exchange. Research suggests that

self-disclosure operates according to what Gouldner (1960) originally termed 'the norm of reciprocity' (Jourard, 1959; Jourard & Landsman, 1960). The norm of reciprocity stipulates that people feel obligated to comparably return the services given to them by others. These services can come in the form of various things, including favours and self-disclosure. Reciprocity of self-disclosure, in particular, refers to the expectation that disclosure will be returned at a comparable level of intimacy. A study investigating this phenomenon conducted by Chaikin and Derlega (1974), involved showing participants videos of two women having a conversation. One woman was the initiator (she started the conversation) and the other was the respondent. The intimacy level (either high or low) of the initiators' disclosure was manipulated, and participants' ratings of liking for the respondent in the videos were then assessed according to intimacy levels. Results showed that liking was influenced by the norm of reciprocity, in that respondents who disclosed at similar levels of intimacy were better liked by participants than those who responded with a discrepant level of intimacy. It appears that perceptions of self-disclosure may be heavily influenced by social norms, and that people may feel they are obligated to return the favour of disclosure. Not only do people feel the need to reciprocate disclosure, but this disclosure is expected to occur at similar intimacy levels.

Social Information Processing (SIP) Theory

Walther (1992) originally developed the Social Information Processing (SIP) theory of computer mediated exchange, which outlines the extent to which people gain information through social communication, and how people use this information to establish impressions of others. He proposed that getting to know someone is based on a

small initial amount of information in text based form, and that relationships develop to the extent that there is information first available. Walther developed this theory to clarify the mechanisms of social interaction online, and went on to explore how one uses the initial available information to develop first impressions in online settings. He argued that while there is a lack of non-verbal cues in computer-mediated communication, this does not necessarily imply that online relationships are any less meaningful or strong as relationships offline.

People are still able to get to know someone based on the verbal cues available online. Walther (1996) suggested that people are inherently good at assessing both verbal and non-verbal cues, and that people can establish affinity (liking) for their online partner, regardless of the lack of non-verbal cues (e.g., gestures). Walther asserted that while computer-mediated relationships develop at a slower pace, they are equally as strong as offline relationships.

The anticipation of future interaction is another important component of this theory, as this motivates people to be more intimate in their disclosures online. For example, people who expect to meet their online partner at some point in the future may be more likely to exchange more relational messages with their partner (Walther, 1996), and motivate people to further develop their relationships.

Social exchange theory, social penetration theory and the reciprocity norm attempt to explain establishment of relationships, however they do not necessarily take into account relationships that are already formed and how these existing relationships function over time. In addition, because these theories for the most part are meant to

explicate social communication offline, they may not map as easily onto online social interaction, and, more specifically, personal self-disclosure online.

The Shift in Social Communication

With the shift in social communication from face-to-face interaction to online communication, theorists have sought to extend their current knowledge of standard theory in offline contexts to an online setting. Walther's (1996) attempt to apply offline theory to online relationship formation resulted in the formation of the online hyper-personal theory. In the following sections, his theory will be reviewed and the implications of existing research in an online context will be explored.

Online Hyper-personal Theory

Following from social information processing theory, Walther (1996) established the hyper-personal theory of online relationship formation. Walther coined this "hyper-personal" because he noted that, in several instances, communication online could surpass the level of intimacy found in parallel face-to-face interactions. This theory applies to relationships formed and maintained solely online, and focuses on electronic communication that is devoted to social or recreational interaction (e.g., chat rooms, social networking). Despite the argument that offline relationships are far more intimate and of a higher subjective quality than online relationships (Sproull & Keisler, 1986), Walther argued that online relationships are at least just as, and in some cases more intimate than relationships offline.

Walther noted that "selective self-presentation" may occur online, whereby senders of information online may opt to convey more favorable aspects of the self. He

identified two elements common in online interaction that may enhance self-presentation: *asynchronous communication* and *reduced cues*.

Asynchronous time (where there is time lag in between messages) allows for careful planning of communication, unlike spontaneous talk where responses are expected almost immediately following the delivery of a message. Walther argued that this form of communication is more relaxed, and thus allows for more efficient allocation of cognitive resources. He cites Ochs's work (1979) on discourse and goes on to assert that "asynchronous verbal communication is more inter-subjective and less egocentric than in unplanned (spontaneous) discourse (Walther, 1996, p. 26). In essence, Walther argued that asynchronous communication may be more socially desirable and effective.

Walther posited that first impressions are highly controlled and manageable in online communication. Because information is conveyed verbally in most cases and often lacks physical cues that users cannot otherwise control, editing and self-censorship occurs more often. As a result, the receiver of the information may over-attribute the reduced cues provided by the sender, and form a more positive image of their partner (Spears & Lea, 1992). Walther explained that this "over-attribution" occurs when the receiver of information builds stereotypical impressions of the partner. Given minimal amounts of information to base impressions on, receivers over-rely on verbal cues in the absence of physical ones, and may idealize the interaction partner.

While this may seem detrimental to relationship formation, Walther concluded that hyper-personal interaction has the potential to be highly rewarding. Quoting

Schlenker (1985), "People are more satisfied in particular relationships and situations to the extent that their desired identity images are supported, validated or elicited" (p. 93).

Disclosure on the Internet

While the majority of studies in this area have focused on self-disclosure in face-to-face contexts (i.e., interviews and case studies), fewer investigations have examined the mechanisms and predictors of self-disclosure in different media contexts (e.g., online, computer-mediated communication). Over the last few years, only a small number of studies have emerged investigating how context plays a role in self-disclosure (e.g., Joinson, 2001; Locke & Gilbert, 1995; Tidwell & Walther, 2002). In order to test this assumption, Joinson (2001) compared levels of self-disclosure in computer-mediated and face-to-face contexts. In addition, visual anonymity and self-awareness were examined as potential predictors of self-disclosure. In Study 1, participants were paired up and were instructed to discuss dilemmas either in a chat room or laboratory face-to-face setting. As expected, participants in the computer-mediated communication setting disclosed more spontaneous personal details (i.e., details about themselves) than those in the face-to-face condition. In Study 2, the same dilemmas and procedure were employed, and a visual anonymity factor was included. To achieve visual identification or visual anonymity, half of the participants were shown a video picture of their discussion partner, and half were not. Results revealed that visual anonymity (i.e., no video image of interaction partner) encouraged higher levels of self-disclosure.

Joinson went on to manipulate levels of private and public self-awareness (high and low). For private self-awareness, video images were transmitted to the participant so

that they were either able to see themselves (high private self-awareness) or a "Simpson's" episode (low private self-awareness) displayed on the screen. For high public self-awareness, participants walked down a well lit hallway and were seated facing two video cameras, encouraging a sense of reduced anonymity. For low public self-awareness, participants walked down a dark hallway to the study room, and sat in a cubicle with no video cameras, encouraging a sense of anonymity. As anticipated, induced high private self-awareness combined with induced low public self-awareness resulted in the highest levels of spontaneous self-disclosure when compared to low private/low public and high private/high public conditions. This study stresses how situations that encourage salient private selves (i.e., high private self-awareness) and lessened public selves (i.e., low public self-awareness) result in increases in self-disclosure. More recent examination of computer mediated communication, in particular instant messaging (IM), showed that even non-anonymous communication (i.e., where public selves are known) online encouraged self-disclosure (Schouten & Valkenburg, 2007).

Tidwell and Walther (2002) looked at the effects of computer-mediated communication on self-disclosure, impressions formed about interaction partners, and evaluations of interaction partners. Similarly to Joinson's study (2001), participants were assigned to either a face-to-face meeting, or a meeting through use of an email system (i.e., they sent email messages back and forth). Results showed that computer-mediated communication participants used more interactive questions and self-disclosed more than did their face-to-face counterparts. In addition, computer-mediated communication users

asked and offered more intimate details. In terms of impressions and evaluations, face-to-face participants initially felt more confident in their partner attributions (i.e., how well they felt they knew their partner) than computer-mediated communication participants, but by the end of the conversation, this difference had disappeared. It could be that initially, face-to-face participants feel more confident in their attributions due to the added benefit of physical cues. As conversations progress, computer-mediated communication users ended up feeling equally as confident in their impressions of their partners, even despite the lack of visual/physical cues, lending support to Walther's theory of online hyper-personal communication. Even despite suggestions that online relationships were not as strong, and that interaction partners online were not able to 'get to know' their partners as well without other more visual or physical cues, these findings imply that the online medium is equally as effective for forming close bonds and positive impressions of interaction partners as offline interactions.

The combined results of studies investigating online interactions highlight how interpersonal communication and self-disclosure may change as a function of whether the interaction takes place online or offline (e.g., Joinson, 2001; Locke & Gilbert, 1995; Tidwell & Walther, 2002). While offering insight into communication online (e.g., email, instant messaging, chat rooms), studies looked at the quantity of information presented and not the specific content, such that they reported how much people disclose, but not on which topics they disclose. For instance, Tidwell and Walther used the proportion of conversations, not the specific topics, to obtain a gauge of how much self-disclosure resulted in each group. In Joinson's (2001) study, intimate conversations were examined,

but were not coded for types of disclosure. Locke and Gilbert (1995) compared perceptions of sensitivity of material, self-disclosure, comfort, and enjoyment across contexts (online versus paper-and-pencil), but did not analyze specific responses. The next step in self-disclosure research is to compare how traditional (paper-and-pencil) and new media contexts (e.g., Facebook) affect people's decisions about how and, more importantly, *what* to disclose or, in other words, which topics in particular people are choosing to share with others. Moreover, in the case of online social networking profiles, a large majority of disclosure is presented by users without the expectation of interaction, such that details are simply displayed for others to view. Therefore, examination of information broadcasted about the self, rather than interactive information sharing where feedback and reciprocal communication is expected merits examination. The Internet offers an anonymous forum for personal communication and, as the Internet becomes an omnipresent aspect of interpersonal communication, we may expect to see an increase in self-disclosure patterns for online contexts (e.g., Henderson & Gilding, 2004).

Personality and Online Communication

Associations between various personality factors and online communication are mixed (Amichai-Hamburger, Wainpel & Fox, 2002; Ross, Orr, Sisic, Arseneault, Simmering & Orr, 2009; Swickert, Hittner, Harris & Herring, 2002). In most cases, studies have employed the Five Factor Model (McCrae, 1992) of personality to examine how various personality traits are related to patterns of technology use and disclosure online. Findings revealed that those with higher scores on neuroticism tended to use the internet more to avoid loneliness (Butt & Phillips, 2002). Researchers suggest that

because these individuals reported lower levels of social support, they may have resorted to online activities to achieve an unfulfilled need with hopes of obtaining support through online interactions. Conscientiousness was negatively related to online communication (Swickert, Hittner, Harris & Herring, 2002). This relationship was explained by a reduced desire to procrastinate, and thus, an active avoidance of distracting tools including online social networking sites. Those scoring higher on extraversion were less likely than their more introverted (lower on extraversion) counterparts to engage in online communication (Amichai-Hamburger, Wainapel & Fox, 2002). Amichai-Hamburger and colleagues (2002) argue that this pattern is dependent on the location in which a person perceives their true identity. They suggest that for those scoring higher on extraversion, true identity resides offline. In contrast, for those scoring higher on introversion, true identity resides online. According to Amichai-Hamburger and colleagues, because true identity resides online those who are more introverted are more likely to use online social networking sites. Wehrli (2008) found that extraversion played an important role in social networking. Specifically, in their sample of 1560 students, extraverts were more likely to sign up for social networking sites, adopted the technology at a faster rate and had larger friends' lists than their less extraverted counterparts. Wilson and colleagues (2010) found that extraverted individuals reported higher levels of social network use. Finally, Ross and colleagues (2009) found that while those higher on extraversion belonged to significantly more social groups on Facebook, scoring higher on this trait was not significantly associated with time spent online or use of certain features of Facebook, such as frequency of status updates. Because findings are mixed, the associations

between personality and use of social networking sites including Facebook require further investigation. While it is possible that personality may impact on the likelihood to disclose, this factor may also be related to the use of other features of the site, including privacy settings.

Familiarity with Technology

Perceived comfort, ease and expertise with computers strongly predict actual use of computers (Mueller, Wood, Willoughby, Ross & Specht, 2008; Spitzberg, 2006). In short, individuals who are more accustomed to and are more comfortable with a technology, also use the technology more frequently. As Lewis and Fabos (2005) have proposed, as time progresses highly competent users may not consciously think about how they are communicating, and instead communicate without hesitation. Because Facebook is such a pervasive communication tool, it is proposed that as familiarity and comfort with the site increases so too does the propensity to disclose information. Aside from disclosure, it is possible that familiarity with technology may or may not predict to use of privacy settings. On one hand, as familiarity and expertise increases, use of all the various features of Facebook, including privacy settings, may increase. Alternatively, if highly competent users do not consciously think about how they are communicating, perhaps they will not be thinking about privacy settings either. This possibility will be explored.

In the following sections, the relation between privacy and self-disclosure will be addressed, followed by an overview of privacy theory offline and online.

Privacy and Self-Disclosure

There is a fine balance between maintaining privacy and emotional distance, and sustaining close, intimate relationships. While it is essential for most people to protect and have control over their personal information, self-disclosing intimate details is a necessary component in establishing and maintaining close, healthy relationships (Altman & Taylor, 1973). *Privacy*, defined as a boundary regulation process that controls the degree of contact one has with others, is strongly linked to self-disclosure. Self-disclosure adjustment can be considered a boundary regulation process, in that increased control over information that is exchanged is related to greater levels of privacy in a social relationship (Derlega, Metts, Petronio & Margulis, 1993). Regulation of interpersonal boundaries dictates the kinds of relationships that are formed (Derlega & Chaikin, 1977), and influences levels of closeness and intimacy within social relationships. In a study examining privacy and disclosure, results revealed that for initial encounters, less private people (low privacy preference) exhibited higher levels of self-disclosure, were more likely to open up to their interaction partner, and felt more comfortable interacting with their partner (Larson & Bell, 1988).

Theories of Privacy

Privacy Offline

Two distinct theories of privacy developed in the 1970s have been established and recognized in the literature (Westin, 1970; Altman, 1975). Westin's (1970) theory of privacy is defined as a boundary regulation process that focuses on the *types* and *functions* of privacy that operate on individuals, groups and organizational levels. He was

interested in understanding and explaining how privacy served to protect the individual from exposure, by temporarily limiting access to themselves by others. Westin identified the ways in which privacy is attained and maintained in everyday life, and posited four states of privacy (how privacy is achieved): *solitude; intimacy; anonymity; and reserve. Solitude* is freedom from the observers' gaze, and can be obtained by sheltering oneself from the public eye. For example, taking a getaway to a remote wilderness retreat might offer solitude and release from the observer. *Intimacy* occurs when a small select group of individuals achieves a close, honest relationship, in which they share personal details with specific close others. *Anonymity* is freedom from identification through censorship of personal information. By controlling what information is presented, one can ensure that their unique identity is not revealed. For example, in the absence of personal information including name and birth date, one remains unidentified, and therefore maintains their anonymity. Lastly, *reserve* is the act of limiting the amount and type of information that is accessible about the self. For example, by choosing to disclose certain superficial details (e.g., hair colour or favorite food) one limits access to private thoughts and more sensitive personal details.

In addition to the mechanisms through which we maintain privacy (how we obtain privacy), Westin went on to distinguish four functions of privacy (the reasons why we need privacy). These functions include: *personal autonomy; emotional release; self-evaluation; and limited and protected communication. Personal autonomy* is the desire to avoid the threat of manipulation, or control by others. *Emotional release* is relief from one's social obligations such as role demands, and emotional states. *Self-evaluation* is the

sense of self-reflection/contemplation and integration of experiences into meaningful lessons learned. Lastly, *limited and protected communication* is composed of two related factors. *Limited communication* refers to setting communication boundaries and restricting accessible personal information, whereas *protected communication* refers to sharing personal information with certain trustworthy others. These states (or types) and functions have helped researchers to develop measures of privacy in various settings (e.g., Marshall, 1974).

Altman (1975) suggested that the functions of privacy (why we need privacy) were hierarchical and that the overarching and most important function of privacy is to obtain a self-identity. His theory of privacy consists of four components, which focus on the process by which people regulate levels of social interaction. The first component is the temporal boundary regulation process, whereby individuals adjust their levels of required privacy depending on the surrounding environment and their own internal state. As time passes, and situations change, people continually adjust their levels of privacy. Second, in contrast to Westin's theory, Altman's theory distinguishes between desired and actual levels of privacy by discriminating between privacy that is required, and privacy that is experienced. Altman proposed that an optimal level of privacy exists, in which our desired levels of privacy match our actual levels of privacy. For example, if someone wishes to have complete privacy with little contact from others and they achieve this, they are at their optimal level of privacy. When this optimal level is not achieved, too much (i.e., isolation) or too little privacy (i.e., crowding) may occur. Altman also suggested that privacy is bidirectional in nature, involving both input (e.g., regulating if

we are observed or not and noise from the environment) and output (e.g., verbal communication/disclosure). Third, similar to Westin's theory, Altman's theory considered that privacy should be applied both to the individual and group level, rather than just from the individual's point of view. Fourth, Altman's theory takes into consideration input as well as output, such that he focused on both how people exercise control over input (e.g., protecting themselves from the observers' gaze) and output (e.g., what types of information they disclose). By taking into account the interaction between these two processes, Altman extended previous notions of privacy to include a more comprehensive overview.

In addition to these four components, Altman incorporated behavioural mechanisms used to regulate privacy (e.g., shutting the door, verbal expression). Inclusion of behavioural techniques (e.g., shutting the door, personal space) used to maintain and regulate their optimal levels of privacy contributes a unique aspect to the existing privacy theory originally set forth by Westin.

While Westin primarily focused on psychological aspects of privacy, Altman went on to highlight the importance of the environment or context in privacy regulation. More specifically, Altman proposed that understanding of the psychological components of privacy required systematic consideration of the social world, interactions between people, the physical environment, and the temporal nature of social relationships (Altman, 1990). Even as Altman's theory has been deemed an "environmental theory of privacy", environment does not always strictly imply physical environment. Environment has been conceptualized in two distinct ways. First, environment has been characterized

as an objective, physical environment in which we move (Margulis, 1977). Second, Wohlwill (1973) referred to the 'environment' as the perceptual, symbolic environment that we construct in our minds. This conceptualization of 'environment' is linked to psychological descriptions of privacy. According to the perspectives of both Altman (1990) and Wohlwill (1973), environment can be physical and/or psychological in nature, and must be addressed when describing definitions of privacy.

Both Westin and Altman's privacy theories address the notion of limited access approaches to privacy regulation. In contrast, Altman highlighted how perceptions of privacy may be specific to one's culture, while Westin referenced privacy in terms of political values. Although both Westin and Altman's theories of privacy offer deep insight into how and why privacy occurs in relational settings (i.e., between interaction partners, in group settings or in an organization), these theories fail to address how privacy occurs in online settings where there is a lack of direct interaction. For example, in the case of personal online profiles, where users display information without the expectation that someone will respond directly to this information, how do the states (how privacy is achieved) and functions (why privacy is necessary) of privacy operate ? What mechanisms are at work in this context? Although Altman went on to describe how people exercise control over both input and output of information, these components are again, specific to offline self-disclosure.

Privacy Online

In an attempt to apply the concept of privacy to online settings, theorists have formulated a newer online privacy theory. Two key theorists in this area are Moor (1997) and Tavani (2007).

Originally introduced by Moor (1997) and later revised by both Moor and Tavani (2001), the theory of "restricted access/limited control" centers around the idea that information is shared with specific people at specific times. Central to the framework of this theory is the idea of control, and more specifically, *limited* control. Both Moor and Tavani acknowledged that in the computer age it is virtually impossible to control one's personal information at all times, and therefore proposed that instead, it is important to ensure that the *right people* have access to certain information at the *right time*. A key component of this theory is the notion of the "situation". A situation can include various contexts that are normally regarded as being private, including relationships, activities in a specific location, or storage, access or manipulation of information in a database. Activities involving the internet can, therefore, be considered situations. Tavani (2007) argues that it is the *situation* in which personal information can be used by others, not the information itself, that dictates whether or not the information should be declared private. In addition, he goes on to say that details about access to personal information should be "completely public" (p. 16) and known to all who are involved. This theory then has great implications for privacy policy construction, highlighting the need for clear and openly communicated roles and responsibilities. With the inclusion of clear policies,

debate over when normative laws should be established to protect online privacy in various situations (e.g., faculty salaries) can be resolved.

While theories of privacy have clarified different mechanisms and components driving the boundary regulation process, less is known about individual definitions of privacy and how they vary. How and why do perceptions of privacy differ, and what influences these differences in perceptions? Do computer experience and usage relate to perceptions of privacy and privacy behaviours? Do personal experiences and the intended (or mental) audience relate to perceptions of privacy and privacy behaviours? Does context play a role in perceptions of privacy and privacy behaviours? Do privacy related behaviours differ when disclosures occur online? It could be that users view their online behaviours as more anonymous and therefore feel as though their information is more private when, in fact, this may not be the case. It is important to consider how people perceive privacy, because these definitions may very well impact on what they choose to disclose and use of privacy settings. Given the relative lack of research assessing self-disclosure as it relates to perceptions and awareness of privacy online, the present research provides an exploratory examination of these issues.

Identity Theft and Threats to Personal Security

Identity theft and personal security are ever-present concerns associated with information disclosed online (e.g., Fogel & Nehmad, 2009; LaRose & Rifon, 2006; Lee, Im, & Taylor, 2008). In apparent opposition to the numerous warnings issued by law enforcement and public awareness groups regarding the need to be cautious in disclosing personal information (e.g., Child Online Protection (COP); McCandlish, 2002; Willard,

2006), one of the primary goals of social networking sites is to encourage disclosure of personal information with others online. This personal information can include full names, addresses, birthday and year, contact information, and photos. Even a select few pieces of personal information, however, has the potential to provide identity thieves with the means to acquire "identity –based" information such as social insurance numbers, credit cards, driver's licenses, etc. With these pieces of information, even more critical legal documents can be procured, such as passports (Sullivan, 2008). Apart from concerns regarding the protection of identity, disclosure of personal information (even if limited) can be sufficient, when combined with other Internet based tools such as reverse directory checks, to secure home phone numbers, full addresses, age and gender and other information that could leave a person vulnerable (Messmer, 2007).

Given the widespread use and potential dangers associated with online communication, a thorough understanding of the features of networking sites, and how people are using these sites is critical in developing ways to educate users about how to protect their information and themselves. The overarching goal of the present research was to gain a better understanding of what can be found in online social networking profiles, specifically, Facebook. Apart from collecting data on the kinds of information users were choosing to include (and exclude) in their personal profiles, the following studies sought to examine the impact of individual characteristics on the type of information that is likely to be present in an online profile (i.e., information that is self-disclosed as a function of characteristics including age, gender and relationship status).

The Current Research: Predictors of Disclosure and Privacy Settings Usage in an Online Social Networking Site.

The Online Social Context

Due to the nature of online media, the social context in which online communication occurs may be fundamentally different from social interactions in offline contexts (e.g., face-to-face). Features inherent in online interaction may encourage or hinder self-expression (e.g., Henderson & Gilding, 2004; Walther, 1996). Researchers have argued that a large proportion of the meaning derived from social communication comes from non-verbal feedback (Argyle, 1975). Given that certain cues are "filtered out" in online communication (Hian, Chuan, Trevor & Detenber, 2004), debate has arisen over the benefits and drawbacks of online social interaction. Though elements such as accessibility and anonymity may encourage users to disclose intimate details about the self, without worry of exposure (Carnes, 2003; Cooper, Shapiro & Powers, 1998), many users are not fully aware that they may be sharing personal information in a public domain. Given that the Internet has been available for public use since the 1990s and the rapid advance in the number of methods for communicating on the net with growth in Internet usage (blog, email etc.) increasing by 146% from 2000-2010 (World Internet Users, 2010), it would be surprising that many users possess a relatively naïve technical understanding of what can and does happen to the information they share on the net. This naiveté may put users in a position of vulnerability. Even long-time Internet users may not understand exactly how the Internet works. Furthermore, amount of experience with online communication may not necessarily imply technical knowledge.

For example, without knowledge of the underpinnings of computer technology and security, users may disclose potentially damaging or very personal/intimate information, without realizing it. It may therefore be useful to assess factors including personality and familiarity with technology, and how these are related to use of technology. Moreover, users' perceptions about communication online, and the factors that influence what they are willing to disclose, such as who users are targeting when disclosing, may be of paramount importance for understanding the predictors of online information sharing.

Roadmap and Overview of the Current Studies.

This dissertation presents four studies. The fours presented are based on data collected from Facebook between the years 2008-2010. Studies 1 A, B and C were archival and looked at the same 400 publicly accessible profiles on Facebook. The main purpose of Study 1 A was to create a comprehensive scoring that could be used to assess the kinds of information disclosed in personal Facebook profiles. Study 1 B utilized the scoring tool developed in Study 1 A to categorize and examine information disclosed in terms of three types of threat: identity threat, personal security threat and the potential for stigmatization. Study 1 C extended Study 1 B by including an examination on all content available to users, rather than just the three limited categories. In both Study 1 B and C, factors that predicted disclosure within the three categories and overall content areas were investigated in an exploratory fashion to gain a better sense of how users were disclosing online.

Study 2 was a three-part experimental study that extended the findings of Studies 1 A, B and C by examining the impact of various factors on the creation of a Facebook

profile. Part 1 investigated experimentally the impact of story, gender of the participant creating the profile and gender of the target person for which the profile was created on disclosure and use of privacy settings. In the current study, in order to obtain a clearer picture of disclosure, it was necessary to control the information disclosed in the profiles. As such, information was fabricated for a target individual, and participant disclosure of information for this target person was examined. Based on privacy policy literature and research highlighting the saliency of anecdotal stories (Stanovich, 2009; Metzger, 2006, Spiekermann, Grossklags & Berendt, 2001), it was anticipated that participants who read a story about personal privacy invasion would disclose less information than those who read either Facebook's legal privacy policy or a story about the history of the internet (control). In addition, having read the privacy invasion story was expected to encourage greater use of privacy settings among users.

In keeping with research examining gender differences in self-disclosure (e.g., Dindia and Allen, 1992), it was expected that female participants would disclose more overall, but that this difference may be dependent on the topic of disclosure (Derlega, Durham, Gockel & Sholis, 1981). More specifically, male participants were expected to disclose more in specific content areas (e.g., activities, views, education). Lastly, given that females are more often the victims of online abuse (WHOA, 2008) it was expected that participants would disclose less about female targets than about male targets.

Part 2 consisted of an exploratory examination of predictive factors such as personality (private and public self-consciousness, extraversion), the virtual audience (i.e., who they had in mind when posted information), perceptions of online privacy,

online privacy attitudes and behaviours and reported self-disclosure on actual disclosure and privacy settings use within Facebook profiles.

Part 3 examined experimentally the impact of the context in which the profile was created, gender of the participant creating the profile and gender of the target for whom the profile was created on disclosure and use of privacy settings. Based on online hyper-personal theory (Walther, 1996) and previous research showing that online media generated higher levels of disclosure (Joinson, 2001; Schouten, Valkenburg & Peter, 2007, Wood, Nosko, Desmarais, Ross & Irvine, 2006), it was expected that participants filling out a profile on paper and pencil would be less inclined to disclose information than their online counterparts. In terms of privacy settings usage as a function of context, no specific hypotheses were set forth. There is no known research examining the impact of context on settings use, and therefore this examination was exploratory in nature.

An Archival Examination of Information Disclosed in Existing Facebook Profiles

Given the vast array of information that can be shared and the number of users, concerns regarding security and privacy issues are a recurring issue (Acoca, 2008). Some concerns involve potential threats to personal safety from the abundance of information that is assumed to be available and accessible about an individual on their online profile. Specifically, there are concerns regarding identity theft if users provide too much information (e.g., birth date, address, phone, full name etc.). In addition, there are concerns for personal safety for vulnerable users who could be stalked, or otherwise threatened. A less commonly considered threat is the possibility of social risk as a

function of self-identification with minority or stigmatized groups. Although some of these concerns have surfaced in the popular media (e.g., news.cnet.com), there is little empirical investigation documenting how much and what kind of information is present in personal Facebook profiles to determine the potential for threats of any type, nor is there any information regarding how users differ in the information disclosed in their profiles to provide clues as to who is most likely to be at risk.

Study 1 A

Creation of a Scoring Tool for Assessing Disclosure in Facebook

The primary purpose of Study 1 A was to develop a scoring instrument to summarize what information could be disclosed on Facebook profiles. To do this, a comprehensive coding tool was required. From this tool, we then examined the frequency for each piece of information to determine what is and is not likely to be found in online profiles.

General Method

Participants. A sample of 400 randomly selected, accessible, personal profiles from 8 Canadian Facebook networks was collected. The networks included 4 community networks (Toronto, Vancouver, Charlottetown and Kitchener) and 4 university networks (Mount Allison University, Memorial University of Newfoundland, University of Toronto and Wilfrid Laurier University). Networks varied in size, ranging from small to large. Small networks contained up to 14000 profiles (39.2 % of the sample), medium networks contained 36000 to 150000 profiles (37.2 % of the sample), and large networks contained 720000 profiles or more (23.6 % of the sample).

Specifically, 12.3% of the sample came from a network exceeding a million people, 11.3% from a network of approximately 720000 people, 15.2 % from a network of approximately 150000 people, 12.2% from a network of approximately 56000 people, 9.8 % from a network of approximately 36000 people, 15.9 % from a network of approximately 14000 people, and 23.3 % from a network of approximately 5000 people.

Of the 400 personal profiles, 328 indicated gender (116 females, 155 males). Additionally, 301 profiles disclosed age. Among the females, ages ranged from 19-47 years (M= 22.90 years, SD = 3.91 years). Males ranged in age from 17-61 years (M= 23.90 years, SD= 5.03 years). The mean age of males and females who reported both their age and gender did not differ, t (269) = 1.73, p = .09.

Procedure

A scoring tool was developed in order to assess the content of the personal profiles. Construction of the scoring tool was a multi-step process. First, a blank template of a Facebook profile was examined to identify potential pieces of information that could be included in a profile. Two raters independently created checklists from this blank profile template. Following these independent content analyses, an aggregated 90 item checklist was constructed which was comprised of all items from both raters. Six independent coders then used the aggregated coding checklist to code actual online Facebook profiles. Each coder noted any items missing from the checklist that would be required to code their profiles. Coders met and discussed content that was not captured by the aggregated coding checklist. Following this discussion a final checklist comprised of 3 identification items (i.e., username link, the network searched, and the size of the

overall network) and 97 dichotomously scored items (i.e., whether the piece of information was present or absent) was constructed (see Appendix B for the complete checklist and descriptions of items, note that the first three items are the identification items).

Once the coding checklist was established, six raters coded the 400 participant profiles. Each coder coded 50 -100 profiles. Networks searched were counterbalanced across coders. Random selection of profiles was achieved using a randomization feature of the Facebook program where 10 profiles are generated at random. These 10 profiles would include profiles that were and were not publicly visible. On average, 50% of profiles that were retrieved were publicly accessible. Coders scanned the 10 profiles and selected the first one from the list of 10 that was publicly visible. The search for profiles was continued until all raters coded their full allotment of accessible profiles. In order to ensure consistency between coders, reliability was conducted on 40 profiles, representing 10% of the data. Percentage agreement was 99%, indicating high inter-coder reliability for the 97 dichotomous items. Differences were resolved through discussion.

Results

Descriptive summaries were calculated for each item on the checklist that was available among the accessible profiles (See Table 1 for a summary). Overall, the fifteen most consistently disclosed/provided pieces of information (available on 63% or more of the profiles) described personally identifying information (i.e., birth date, gender, profile pictures, photo albums, tagged photos and general photos of the user) as

well as social connections (i.e., groups joined, and friends viewable). In addition, education information (college/university attended) and regular update information (status, wall and mini-feed) were included. Finally, playful communications such as acceptance of pokes, messages, and gifts, and applications were frequently provided. In contrast, the fifteen least frequently included items (9% or less) described key personal information (Zip/Postal Code), phone numbers (both land line and mobile), home address, city or town, website and former name. In addition, there was also a limited amount of information provided regarding some aspects of educational experience (i.e., school mailbox, courses, degree, awards, and room). Finally, optional "wall features" (i.e., Super Wall and Advanced Wall), market place listings and events as described in the mini feed were also infrequently included. Of the 97 items that could be dichotomously scored, 26 items were disclosed by at least 50% of the sample (see Table 1 for summary).

Discussion

Two important outcomes were apparent from the descriptive summary of Facebook profile content. First, despite the potential for significant disclosure through these online social networking profiles, on average, people were choosing to display approximately 25% of possible information for other users to view. This clearly indicates either a reticence to invest heavily in developing online profiles, or active decisions to limit disclosure. Interestingly, the pieces of information that were disclosed were neither consistently "safe" nor "unsafe". Specifically, for both the most prevalent and least prevalent pieces of information included, there were highly personal pieces of

information. That is, in some cases profiles contained the most salient pieces of information required for identity theft and personal safety threats including identifying pictures, birth date, and regular mini-feed updates. These pieces can be used to obtain social insurance numbers and physical location, posing both identity and personal safety threats (Messmer, 2007). However, equally critical pieces of information viewed by the police as particularly risky and pertinent to identity theft such as land and mobile phone numbers and zip/postal code were not readily apparent. Although it makes sense that features such as walls might be less frequently present because these features require active creation and generation to establish and maintain, it is surprising to see information that is prompted being selectively included/disclosed. Therefore, users are demonstrating some discretion regarding what kinds of revealing information they are willing to share. In keeping with Westin's theory of privacy (1970), it appears that even online, users still maintain certain levels of anonymity and reserve by limiting disclosure of certain pieces of information, albeit there are inconsistencies in the information provided. Specifically, users with publicly accessible profiles are, at the same time, choosing to display and censor personal information that can be considered risky.

In an attempt to understand who is likely to include revealing information and what types of information are likely to be produced together, two additional studies were conducted.

Study 1 B

Assessing Three Types of Information Threat on Facebook: Personal Identity, Personal Security and Potential for Stigmatization

With a rapid rise in popularity and use, online social networking sites have introduced new and potentially harmful ways for individuals to access personal information. Identity theft and personal security threats are ever-present online, and thus calls for research examining specific kinds of information disclosed online that may pose a particular risk to the user (Acoca, 2008). Two kinds of threats are possible. One deals with identity theft, which occurs when personal information is used to commit a crime or theft (e.g., impersonation) without the discloser's consent and/or knowledge. Full names, addresses, phone numbers and birthdates are all pieces of information that can be potentially harmful to the discloser if used the wrong way, because other potentially harmful information (e.g., social insurance numbers, credit card information) can be accessed through indirect means using these core pieces of information (Acquisti & Gross, 2009). Another kind of threat is social threat or potential danger to the self and/or group(s) that an individual belongs to. Information such as contact information, sexual orientation, group membership, religious affiliation, and political affiliation are all details that can potentially be used to harm and stigmatize an individual. In this second study, we explored means for examining identity threat, personal and group threats.

Method

Materials and Procedure. Three disclosure categories were developed through qualitative analysis (Patton, 2001). All individual items were considered and based on

these items, categories were generated. Any discrepancies were compared, discussed and resolved by discussion. Development of each of the three categories is explained in further detail in the sections below. The first category reflected personal identity information, the second involved sensitive personal information, and the third involved potentially stigmatizing information. Refer to Table 2 for category descriptives.

Personal Identity Information (Default/Standard Information). The first category involved revealing basic personal identifying information, or what was deemed default/standard information. This information was defined as details people might disclose in banks, schools, jobs etc., but that could be used in potentially threatening ways.

To develop this category a three stage process was used. First, two researchers conducted a content analysis of the 97 items in the full checklist. The number of items was first reduced based on frequency. Items that were very infrequently disclosed (less than 5% of users disclosed the information) were omitted. In addition, items that lacked variability or did not cohere with the other items were omitted. Items were further reduced based on whether the item did or did not reveal default or standard personal information that is typically required to identify a person. Items that failed to meet this requirement were omitted. Next, separate from the sample of 400 profiles, 18 research assistants with experience working in psychology labs examining technology and technology applications in daily life, were recruited to participate in a pilot study to construct the final category of standard/default information. First, these research

assistants were asked about their familiarity with Facebook through two questions. Specifically they were asked to use a 7-point Likert-type scale (1= not at all familiar with Facebook, 7= extremely familiar with Facebook),

"Please rate on the 7 point scale below how familiar you feel you are with Facebook".

Among these research assistants the level of familiarity with Facebook was relatively high (M = 5.67, *SD* = 1.82), however, scores ranged from 1 to 7.

The research assistants were also asked about their log in behavior. Specifically, they were asked,

"On average, how often do you log into Facebook in a one-week period?"

On average, the majority of research assistants logged into Facebook multiple times per week (M = 19.17, *SD* = 22.92), although the range from 0 to 85 times per week was variable, with two participants never signing in. The majority of participants (50%) indicated that they logged in between 12 and 15 times per week.

The research assistants were asked to use the checklist to respond to one question. Research assistants were asked to indicate (with a checkmark) which items they felt were standard or default requirements for the construction of a personal profile or information typically required on personal profile websites. Specifically participants were asked,

"We are trying to determine what pieces of information people consider to be "standard" or typical information requested on personal profile sites. We would like you to look

through the list below to identify the elements that you believe are customarily required in online profiles?"

Items from the checklist that were positively identified by more than 50% of the assistants were considered for inclusion in the scale. Five items were identified as default or standard by more than 50% of the participants. The items and percentage endorsement included: gender (83.3%), birth day (61.1%), birth year (72.2%), email (61.1%), and profile picture (55.6%).

Third, consultation with a local police department and police college was conducted to gain insight into which items were viewed by the police as particularly risky and pertinent to identity theft. Through consultation, 3 additional items (i.e., street address, city /town, postal code) were added to the default/standard information scale. These items identified personal information that could be used in potentially harmful ways.

Finally, this yielded an 8 item default/standard information scale, comprised of street address, city /town, postal code, gender, birth day, birth year, profile picture and email (possible scores ranged from 0 - 8). Higher scores indicated higher levels of self-disclosure for default items.

Sensitive Personal Information (Personal Security). The second category reflected personally revealing/sensitive information. This information was defined as details that could be used to locate an individual, and could be used to threaten or harm another.

To develop this category, two researchers conducted a systematic thematic analysis of the checklist items to determine which variables should belong in the sensitive information category based on the nature of each variable and the potential danger in disclosing each item. After all items were considered, and through discussion, the following were placed in the sensitive information category: email, employer, job position, status, mini-feed, regular wall, profile picture, photo albums, self-selected photos, tagged photos, message, poke, send a gift, and friends viewable (possible scores ranged from 0 -14). Higher scores indicated higher levels of self-disclosure.

Potentially Stigmatizing Information. The third category reflected sensitive personal information that could result in stigmatization within society.

To develop this category two researchers conducted a systematic thematic analysis of the items to determine which variables should belong in the stigmatizing (as well as sensitive) category based on the nature of each variable and the potential for stigmatization of the user by viewers. After all items were considered, and through discussion, the final scale was comprised of religious views, political views, birth year, sexual orientation, photos, friends viewable, interests, activities, favorite music, favorite movies, favorite TV shows, favorite books, favorite quotes, and about me (possible scores ranged from 0 -14). Higher scores indicated higher levels of self-disclosure.

Results

Analyses based on the full sample of 400 profiles explored whether any differences in self-disclosure emerged for profile information. Analyses consisted of 15 independent t-tests with 5 t-tests for each of the grouping categories (default/standard

information, sensitive personal information, and potentially stigmatizing information). Comparisons assessed potential differences as a function of network type (university vs. community), gender revealed (indicated/not indicated), gender (male vs. female), relationship status revealed (indicated/not indicated), and age revealed (indicated/not indicated). Using a Bonferroni correction, the probability for each comparison was corrected to $p < .003$ to accommodate the number of tests conducted. Examination of variables dealing with relationships and with age was carried out using multivariate analysis of variance (MANOVA) and regression analyses. Refer to Table 3 for a summary of analyses.

Comparisons among Network, Gender Revealed, Gender Identified, Relationship Status Revealed, and Age Revealed. Overall, within each set of 5 t-tests, the same three comparisons were statistically significant. Specifically, users who provided information about their gender (present or absent), relationship status, and age[1] disclosed more default/standard information, more sensitive personal information, and more potentially stigmatizing information in their online profiles than their peers who did not disclose their gender, relationship status or age (smallest $t(1, 398) = -2.81$, $p = .005$). See Table 3 for a complete summary.

Relationships Status (single, in a relationship, status not indicated/missing). For each of the three grouping categories (i.e., default/standard information, sensitive

[1] To avoid redundancy, the default/standard information scale was revised, and birth day and year were omitted from the scale for the analysis examining age as a predictor.

personal information, and potentially stigmatizing information), a multivariate analysis of variance (MANOVA) was conducted to compare the amount of disclosure of default/standard information, sensitive personal information, and potentially stigmatizing information as a function of one of three relationship status possibilities (single, in a relationship, missing)[2]. Relationship status served as the between subjects factor.

Results for the default/standard and sensitive personal information categories provided similar outcomes. Specifically, there was a significant main effect of relationship status condition (F (2, 397) = 15.37, $p < .001$ and F (2, 397) = 12.85, $p < .001$, for default/standard information and sensitive personal information, respectively). Tukey-b post hoc comparisons revealed that users who indicated their relationship status as either single or in a relationship disclosed significantly more default/standard information (*Msingle* = 3.34 & *Mrelationship* = 3.11) and sensitive personal information (*Msingle* = 10.12 & *Mrelationship* = 10.08) than users who did not indicate their relationship status (*Mmissing* = 2.54 and *Mmissing* = 8.94, for default/standard information and sensitive personal information, respectively).

Although the analysis for stigmatizing information also yielded a significant main effect of relationship status condition (F (2, 397) = 14.46, $p < .001$), the Tukey-b post hoc

[2] Only two statuses (i.e., single and in a relationship) and status missing (did not indicate their relationship status) were used in these analyses due to very small cell numbers (largest n < 19) for the remaining four statuses (i e , married, engaged, it's complicated, in an open relationship).

comparisons revealed that all three relationship statuses significantly differed from one another. Single users ($M = 8.61$) disclosed the highest amount of this grouping of information in their profiles, followed by users in a relationship ($M = 7.16$), and finally, users who did not indicate their relationship status disclosed the least amount of stigmatized information ($M = 6.03$). See Figure 1.

Analysis of Age. Three linear regressions were conducted to explore whether age predicted disclosure of information for each of the three categories (default/standard information, sensitive personal information, and potentially stigmatizing information). The default/standard information was altered for this analysis through the removal of birth day and birth year in order to prevent redundancy in this measure. Age was entered as the predictor variable, and the new default information aggregate scale was entered as the dependent variable. The overall model was significant in all three cases, $R^2 = .06$, $F(1, 289) = 18.53$ $p < .001$, $R^2 = .08$, $F(1, 289) = 11.31$ $p < .001$ and $R^2 = .08$, $F(1, 289) = 25.74$ $p < 001$, for default/standard information, sensitive personal information, and potentially stigmatizing information, respectively. In all three cases, as age increased, the amount of information presented in personal profiles decreased ($\beta = -.25$, $p < .001$, $\beta = -.19$, $p = .001$, and $\beta = -.29$, $p < .001$, for default/standard information, sensitive personal information, and potentially stigmatizing information, respectively).

Discussion

In summary, all three disclosure categories were relevant, in that all were sources for disclosure and potentially sources for threat. The results revealed a similar trend for all three grouping categories (i.e., default/standard, sensitive personal information, and

potentially stigmatizing information). Facebook users who were acknowledged to have included information about their gender, relationship status, and age, disclosed more information in all three disclosure categories than people who did not indicate this information at all. Further, users who indicated they were single had the highest number of stigmatizing items, followed by users who were in a relationship, and finally, users who did not specify a status had the lowest number of stigmatizing items. This trend was not present for default/standard information or sensitive personal information. Instead, users who were single or in a relationship did not differ on their disclosure of default/standard information or sensitive personal information, but users who did not indicate a status had less of this information in their online Facebook profiles. Individuals at greatest risk for threat could therefore be those who are seeking a relationship. It could be that those who are searching for romantic relationships are using online media as a way to self-present or to advertise themselves to potential dating partners. In fact, research has shown that a large majority of people looking to date use the Internet as a means for finding a partner (Madden & Lenhart, 2006). Online daters not only disclose more intimate details, but disclose these details at a faster pace than do offline daters (Rosen, Cheever, Cummings, & Felt, 2008). While disclosing details online may be necessary to attract a potential mate, there is clearly greater potential for harm.

Interestingly, the type of network and whether the profile was generated by a male or female did not have an impact on whether or not information appeared in a Facebook profile. That is, in the community and university samples, and males and

females did not differ in the amount of information disclosed in their online profiles. While females are generally high disclosers when compared to males in more traditional social interactions (Dindia & Allen, 1992), perhaps males feel more comfortable disclosing in an online setting where there is less pressure to conform or adhere to strict social rules and male stereotypes for disclosure.

Lastly, for those users who included information about their age, as age increased, disclosure of all three types of information (default/standard, sensitive personal information, and potentially stigmatizing information) decreased. Older individuals may be more cautious when disclosing details about themselves. It could be that a greater amount of life experience has taught older users to be wary of information sharing, and they may be more aware of some of the risks involved in disclosure of personal details. For the younger generation, disclosing personal information across a variety of domains (e.g., school, online) is part of everyday life, and may have begun to reduce the gap between private and public selves. Thus, younger people may be less cautious when disclosing highly personal details and feel more comfortable with online disclosure (Goodstein, 2007). Alternatively, it is also possible that as age increases, disclosing certain types of information may not be seen as appropriate. For example, in Western society it is social custom that one does not ask older people for socially revealing information as a mark of respect (Man, 2007). Yet another possible explanation is that social communication that is asynchronous yet personal, such as online social networks, may not provide the forum for communication that is comfortable for older users. While older people may be open to technology, they use it

less (Bucur, Renold, & Henke, 1999), and coupled with a greater awareness of the risks associated with use of technology, may prefer different media for social connections. These interpretations must be considered in light of the fact that the age of non-disclosers is not known, and therefore conclusions about age patterns for this population are not possible.

In summary, although Study 1 A indicated that there were inconsistencies such that some pieces of personal and revealing information were disclosed and others were not, the results from Study 1 B provided an initial understanding of potential individual differences that predict who is most likely to disclose what information. It should be noted that assessment of the veracity of the information presented online was not possible, and therefore the possibility remains that while individual differences predicted disclosure, it is hard to know whether or not these differences were real differences, or simply fabricated by the user (e.g., creating/using a fake gender and age). In keeping with self-presentation theory (e.g., Goffman, 1959), it would not be surprising that some of the users did not display accurate personal information. In some cases this information may have been completed fabricated and in others, as in the case of self-presentation, it is possible that the information displayed reflected an idealized version of the true self. In addition, Study 1B examined only publicly accessible profiles, and therefore patterns of disclosure may be different for profiles that do not allow public access. Study 1 C further explored variables that explain what is disclosed and by whom.

Study 1 C

Examination of Disclosure across Various Content Areas within Facebook

One concern in Study 1 B was that only limited information was examined. Study 1 C provided an examination of all of the content available through Facebook in order to better understand how to conceptualize the information that can be provided and who is likely to disclose it.

Method and Results

The sample included the 400 profiles specified in Study 1 A and employed the same checklist.

A fourth grouping strategy was conducted to include all information present in Facebook but to organize it in a meaningful way. The process involved several steps. First, information was sorted as a function of the layout of the Facebook profile template. However, the template organization tended to include information that was not obviously related thematically. Two researchers carried out discussion about how to categorize information based on thematic coherence. Through discussion, the following 10 categories were identified: Personal information, Relationship information, Age information, Contact information, Education information, Work information, View information, General Picture information, Message and Poke acceptance (whether or not users allowed other users to send them private messages and to poke them), and Wall and Update Information (i.e., regular wall, advanced wall, super wall, fun wall, mini-feed, and status).

A principal components factor analysis with a Varimax rotation was conducted to confirm these categories and the relationships between these variables. The factor analysis yielded 11 factors with Eigenvalues greater than 1.00, which accounted for a total of 66.74% of the variance. Overall, the factors corresponded with the thematic analysis of the two researchers with the exception that one category identified by the researchers was divided into two categories through the factor analysis. Initial Eigenvalues ranged from 1.04 to 6.60, and indicated that the factors explained 16.93%, 9.62%, 8.20 %, 6.13 %, 4.80%, 4.54%, 4.31%, 3.50%, 3.08%, 2.96%, and 2.68% of the variance, respectively. The factor loading matrix is presented in Table 4. The following eleven aggregate scales were created based on the factor loadings and were used in the subsequent analyses: Personal information, Tagged and Self-selected Photos and Update information, Work information, Education information, Message and Poke Acceptance (whether users allow for receipt of private messages and nudges from other users), Album and Profile Picture information, Age information, Contact information, View information, Other Wall Presence, and Relationship information. Higher scores indicated higher levels of self-disclosure for these items. Reliability was conducted for scales that had more than 3 items using Cronbach's alpha[3]. The alphas ranged from moderate to high: .91 for Personal information (8 items), .90 for Work information (4

[3] Cronbach alphas for scales consisting of only three items were low. Alpha levels were .48 for contact information, and .57 for album and profile picture information. Inter-item correlations were carried out for scales with 2 items. Item correlations were 37 for view information, .34 for wall information, and .34 for relationship information.

items), .76 for Education information (4 items), and .84 for Tagged and Self-selected Photos and Update information (5 items). Refer to Table 5 for a list of items in each scale and means.

Following the analyses in Study 1 B, t-tests were conducted first to explore possible differences as a function of network type (university vs. community), gender revealed (indicated/not indicated), gender (male vs. female), relationship status revealed (indicated/not indicated), and age revealed (indicated/not indicated) for each of the 11 topic scales. Given the number of comparisons conducted, a Bonferroni correction was employed and the alpha level for each test was set to .005. These t-tests were followed by a multivariate analysis of variance (MANOVA) looking within relationship status, and finally, with a linear regression using age. Refer to Table 6 for a summary of the t-test statistics.

Type of Network. One out of 11 t-tests was significant. Results revealed that users who belonged to a community network were more likely to include view information in their personal profiles than were their university network counterparts.

Gender Revealed (indicated/not indicated). Five out of the 11 t-tests were significant. Results revealed that users who indicated their gender, also had higher levels of disclosure for: personal information, tagged and self-selected photos and update information, education information, album and profile picture information, and age information.

Male vs. Female. One out of the 11 t-tests was significant. Results revealed that males expressed more information about their political and religious views than did females.

Relationship Status Revealed (indicated/not indicated). Five of the 11 t-tests were significant. Overall, disclosing one's relationship status was related to higher levels of disclosure of various topics, including: personal information, tagged and self-selected photos and update information, album and profile picture information, age information; and view information.

Age Revealed (indicated/not indicated). One of the 10 t-tests was significant. Users who disclosed their age also disclosed more education information.

Analysis of Relationship Status. A multivariate analysis of variance (MANOVA) was conducted with the relationship status condition (single, in a relationship, missing) as the between subjects factor and the 11 aggregate scales as the dependent variables. Results revealed a significant main effect of relationship status condition for 8 of the 11 scales including: personal information (F (2, 397) = 7.20, p = .001); tagged and self-selected photos and update information (F (2, 397) = 8.45, p < .001); album and profile picture information (F (2, 397) = 12.40, p < .001); age information (F (2, 397) = 10.94, p < .001); work information (F (2, 397) = 5.80 p = .003); view information (F (2, 397) = 5.88, p = .003); relationship information (F (2, 397) = 18.91, p < .001) and super fun wall information (F (2, 397) = 5.88, p = .003).

For personal information, Tukey-b post hoc comparisons revealed that single users (M = 4.51) indicated significantly more personal information than did users who

were either in a relationship ($M = 3.36$), or who did not disclose their relationship status ($M = 3.04$).

According to Tukey-b post hoc comparisons, tagged and self-selected photos and update information, album and profile picture information, age information, and work information all yielded consistent patterns. In general, users who either indicated they were single or in a relationship, disclosed significantly more information related to these topics than did users who did not disclose their relationship status. Refer to Table 7 for means.

For information pertaining to religious and political views, Tukey-b post hocs showed that single users ($M = .85$) had significantly more information present in their profiles than did users who did not indicate their relationship status ($M = .52$). Lastly, for relationship information, all three groups differed significantly from one another. Users who were single ($M = 1.06$) displayed the most relationship information, followed by users who were in a relationship ($M = .78$), and finally, users who did not disclose their relationship status were the least likely to display relationship information in their online profiles ($M = .50$). See Figure 2.

Analysis of Age. Ten linear regressions were conducted to explore how age as a continuous factor was related to disclosure of information online. Given the number of regressions conducted, the alpha level for each test was set to .005. Age was entered as the predictor variable, and each of the aggregated topic scales were entered as the dependent variables. For 5 of the 10 scales, age significantly predicted disclosure of topic. The overall models were significant for the following scales: personal information

($R^2 = .04$, $F(1, 289) = 14.11$ $p < .001$, $\beta = -.22$, $p < .001$); Tagged and Self-selected Photos and Update information ($R^2 = .05$, $F(1, 289) = 16.46$ $p < .001$, $\beta = -.23$, $p < .001$); education information ($R^2 = .04$, $F(1, 289) = 10.82$ $p = .001$, $\beta = -.19$, $p = .001$); Album and Profile Picture information ($R^2 = .09$, $F(1, 289) = 28.24$ $p < 001$, $\beta = -.30$, $p < .001$); and relationship information ($R^2 = .07$, $F(1, 289) = 20.78$ $p < .001$, $\beta = -.26$, $p < .001$). Overall, as age increased, disclosure of these topics decreased.

Discussion

For the most part, the outcomes of Study 1 C support the outcomes reported in Study 1 B. Specifically, gender (male versus female) and network membership (community versus university) were not important variables for distinguishing who would or would not be likely to disclose information. Differences existed only for one topic. Unlike traditional face-to-face interactions (Dindia & Allen, 1992), online social networking profiles may provide a means of communicating that facilitates disclosure among males to the same level as evidenced in females. Also, whether an individual belongs to a university-based or community-based network did not strongly predict to the amount of disclosure of information, with the exception of one topic. Apparently, both university and community samples share similar knowledge or attitudes toward revealing information online.

Like Study 1 B, results from Study 1 C revealed that voluntarily providing personal information related to gender, and relationship status was related to greater disclosure of certain topics (i.e., for 5 of the 11 scales). One notable difference between Study 1 B and Study 1 C concerns revealing personal information related to age. In

Study 1 B, revealing any information about age (i.e., whether they indicated their age or not) had an impact on the likelihood to disclose information. In contrast, for Study 1 C, whether an individual supplied information regarding their age or not did not predict information disclosed. Out of the possible 10 topic categories, revealing age was only significant for one (i.e., education information).

On the other hand, in both Studies 1 B and C, when individuals provided their age, it proved to be an important factor in distinguishing levels of disclosure online. As age increased, self-disclosure decreased on 5 out of 10 scales in Study 1 C (i.e., photo album information, relationship information, personal information, Tagged and self-selected photos and update information, and education information) and for all categories examined in Study 1 B. Items in these particular 5 areas tended to overlap with the items in the three grouping categories used in Study 1 B relative to the 5 areas that were not significant in this analysis.

Consistent with earlier discussions, older adults may be less likely to reveal information due to less familiarity and trust with technology or due to more experience, wariness or social prohibitions regarding disclosure of private information (Bucur, Renold, & Henke, 1999; Mann, 2007). In keeping with the norm of reciprocity (Gouldner, 1960), it may be that there is a disclosure "culture" whereby peers within the same age group or social sphere grow to expect certain levels of reciprocal disclosure, therefore encouraging or discouraging information sharing. Perhaps for younger users who have publicly accessible profiles to start off with, disclosure norms are higher,

whereas for older users, disclosure norms set out by their "culture" are lower in comparison. Again, these conclusions apply only to publicly accessible profiles.

Relationship status was very important in distinguishing levels of disclosure for the different topic categories. Overall, those seeking a relationship were far more inclined to disclose on a variety of topics including views, relationship information, and personal information than were their counterparts who were in a relationship or who did not disclose a status. The current outcomes highlight the importance of relationship status for identifying those users who are more likely to reveal highly personal information. Those seeking a relationship may be using Facebook as a less overt dating site, and, thus, may be differentially motivated to disclose highly personal information across a variety of topics regardless of the dangers or threats associated with disclosing this information. Motivation therefore may prove to be an important factor, and merits further investigation in future studies.

Interestingly, contact, other wall information (i.e., Fun Wall, Advanced Wall and Super Wall), and acceptance of messages and pokes yielded non-significant results. In the case of acceptance of pokes and messages, a very high percentage (99.3% and 99% for pokes and messages, respectively) of users had these features present in their profiles. It may be that because these features are a prompted or automatic feature present in a Facebook profile, less variability may result for these particular items. Alternatively, these may also be perceived as more "playful" and social opportunities to interact and may not carry any perceived threat in having them as part of the profile. For other wall information, those that occurred in less than 10% of the profiles, there might

be less use as a function of the amount of effort and time required to generate the materials required to develop these features.

Interestingly, items involving contact information did not result in any significant outcomes as a function of age, gender, network, or relationship status. Perhaps this is a function of the acknowledgement of the high sensitivity of this information with this information being reported very infrequently. Given the many other alternatives for communicating with someone in the social network, including sending a wall post, these other alternatives may be accepted more readily than highly sensitive personal information because these former alternatives leave the door open for connection without exposing oneself to information theft or invasion. Thus, it appears that regardless of group membership, people did not voluntarily disclose this information.

Understanding What is Disclosed

In order to make meaningful conclusions about the data found in the publicly accessible profiles, grouping procedures were used to aggregate various items within descriptive or associated categories (i.e., default/standard, sensitive personal and potentially stigmatizing, as well as according to specific topics). While the same effects were being interpreted in both Study 1 B and C, the different grouping strategies permitted a novel, exploratory examination of the impact that individual difference factors have on disclosure. For the most part, age and relationship status were salient in describing who would or would not be likely to disclose information, while traditional variables such as gender were not significant. In fact, across the grouping strategies

there was considerable overlap in outcomes suggesting that some types of information were particularly salient for some groups.

Overall, this research was important because it provided evidence that highly personal, sensitive, and potentially stigmatizing information is being disclosed in publicly accessible profiles on social networking sites such as Facebook. However, findings also depict users who are expressing discretion regarding at least some personally revealing information. In light of the prevalence of online identity theft, and social threat issues, the results of this study can be used to partially support the need for developing programs and interventions that further caution users of online social networks against placing themselves at risk, especially in the case of those who are not employing basic settings. In addition, Study 1 C provided insight indicating that, in the case of publicly accessible profiles, some pieces of personal information may be more likely to be grouped together, as supported by factor analysis of topic. Examination of profiles that are not publicly accessible would therefore enhance our understanding of disclosure in online social networking profiles.

Study 2

An Experimental Examination of Stories as a Mechanism for Increasing the Use of Privacy Settings in Facebook and Potential Contributing Predictors.

Some level of disclosure is a requirement to participate on social networking sites. As a result, users who otherwise would not disclose personal information may feel compelled to disclose information as a function of the way social networking sites are constructed (Joinson, 2008). For example, in the case of Facebook, users are required to

disclose at least a few key pieces of personal information (e.g., name, birth date and valid email address), as part of constructing an account. The concern with even this small amount of disclosure is that this particular constellation of information, if provided in a public forum, opens the discloser to the potential risk of privacy invasion. Even despite the possibility that users may choose aliases and submit false personal information upon sign-up, the possibility remains that a substantial proportion of users are signed up on Facebook based on their actual information. Therefore, examining mechanisms which might minimize risks associated with disclosure was a key motivation for the present study.

Design and Rationale for Study Two

The focus of this study was threefold. First, the study examined the impact of having individuals read stories about safety and privacy issues as a potential means for reducing the amount of disclosure and increasing the use of privacy settings. The specific design involved two story conditions and a control condition. One story group read privacy information prepared by online social networking site developers and the other group read about a personal case of stalking which resulted from too much disclosure online. The control condition read general information about the history of the Internet that did not raise issues related to privacy or disclosure. It was expected that a simple story manipulation alone might not change disclosure behaviours or use of privacy settings, therefore the second focus was to identify other potentially important variables that might impact on what was or was not disclosed and that might also impact on the story conditions. Specifically, gender and the target person were included.

Participants in the study generated a Facebook account for another person, and the gender of that Facebook target person was manipulated. It was made very clear to participants that this target person was in fact a real person who had provided their personal information for the study. In addition, to further emphasize the presence of the target person, participants were told that the person for whom they were creating the profile may have the chance to view the profile once it was completed. In addition to the target person, the study also addressed the target audience for the Facebook profile. Specifically, the notion of who the account was being constructed for was tested through some preliminary questions targeting the "virtual other". In addition, personality and computer use variables were examined as potential predictors. These variables were added as an exploratory investigation. Finally, the third focus followed from previous research which suggests that the media (electronic versus hard copy) may generate different behaviours. To extend this to a social networking context, half of the participants constructed the new Facebook accounts online and half created them using paper-and-pencil replicas of the sites. Rationales for these specific manipulations are outlined below.

Background: How Can Users Protect Themselves and Others?

Although the system design of Facebook requests users to disclose potentially risky information, the system design also includes features which would allow users to protect themselves and others with whom they connect from privacy threats. Specifically, Facebook gives users the opportunity to change privacy settings for their personal profile information, photo, and video information. Users can also control who

can contact them, who can see their profile and can limit third party access to their personal information. Alternatively, users may also keep an "open" profile, allowing anyone to freely browse through their information. If a user is particularly open with their information and does not change available settings, the default option is to have their profiles entered into search engines such as Google and Yahoo. While this option is selected, a simple Google search of a users' name will pull up their profile and list it in the search results. Online sites have taken steps to educate users and help them to protect their personal privacy. Privacy policies are in place to educate users about their privacy rights and the rights of the site and how information is shared and used by the company.

Privacy Policies and Settings: What Impacts When They Are Being Used?

Although privacy features protect the user and any information that the user may have posted about other people (e.g., pictures, posts, and personal details), many users do not employ available privacy settings, nor do they read the privacy policies (Berendt, Gunther, & Spiekermann, 2005; Milne & Culnan, 2004). Gross and Acquisti (2006) found that the majority of Facebook users did not employ the available privacy settings, allowing for complete access to their profiles, even when they knew about the settings. If any settings were used they were minimal, and allowed, for example, friends of friends or a user's entire network to view their profile. Most people, however, express concern about their privacy, both offline and online (Cranor, Reagle, & Ackerman, 1999; Nosko, Wood, & Kenney, manuscript in preparation; Statistics Canada, 2009). While the general consensus is that privacy is important (Acquisti & Gross, 2006), there appears to be a discrepancy between attitudes and behaviours (Acquisti & Gross, 2006;

Metzger, 2006; Spiekermann, Grossklags & Berendt, 2001). The following section explores this discrepancy further by examining variables that could influence users' decisions to employ privacy settings.

Presentation of Privacy Policies

Given that online privacy is a concern for most users, it is surprising that most do not read the privacy policies. One concern is that the privacy policies may not be presented in a user friendly way. Specifically, the language used may be too "legalistic" or formal to be accessible to most users. Indeed, research has found that, even when users do read the privacy policies many do not fully understand what they have read (Berendt, Gunther, & Spiekermann, 2005; Milne & Culnan, 2004). Legal privacy policies frequently contain wordy, incomprehensible statements (Jensen & Potts, 2004), with readability levels of the majority of privacy policies falling above the capacity of most adults (Anton, Earp, Bolcini, Jensen & Stufflebeam, 2003). Language constraints may, therefore, be an important consideration in understanding why users do not understand and hence, do not utilize the privacy policy information. In addition, especially challenging text that does not inherently appear to be personally relevant, may serve as a deterrent but also may simply be less interesting especially in a media environment where many more attractive visual stimuli are available. In summary, complex text, along with text only presentation may lead users to by-pass reading policies entirely or to terminate their reading shortly after starting. This presents a challenge to policy makers, and perhaps calls for a more engaging and easily understood alternative. In the present study, reading a short yet representative subsection of a formal

privacy policy statement was required prior to completing a Facebook profile. Reading this type of information may encourage less disclosure and greater use of privacy settings.

Saliency of Anecdotal Stories: The Decision to Employ Settings

The power of anecdotal storytelling is robust in decision making research (e.g., de Wit, Das, &Vet, 2008; Fagerlin, Wang & Ubel, 2005; Hamill, Wilson, & Nisbett, 1980; Stanovich, 2009). Humans are natural story tellers (McAdams, 1993, 2001), and prefer personal stories to other forms of data (Kida, 2006) due to ease of processing, retrieval and mental vividness of stories (Hamill et al., 1980; Stanovich, 2009). The power of anecdotal stories for learning has been demonstrated in educational contexts. Anecdotes have proved useful for engaging students during lectures by enhancing interest and encouraging meaning making and greater recall (Bruner, 1996; Cosmides, 1989). This positive impact of personal stories also has a negative counterpart in which personal stories can overshadow more reliable and accurate sources of information (Stanovich, 2009). For example, people may accept the account of one personal story even when it contradicts a body of consistent research findings. This highlights the importance of personal anecdotal stories and their potential impact on employing privacy settings. In the present study some participants were provided with a brief anecdotal story relaying a stalking situation following too much disclosure online. It was expected that the presentation of a salient, vivid anecdotal privacy story may address both the issue of getting people to read privacy related documents, while at the same time persuading them to use the available privacy features. In addition, it may be that a

well told anecdotal story may prove more persuasive than even the most convincing statistical or legal information.

Gender Differences in Online Privacy Attitudes and Behaviours

Various studies have noted gender differences in terms of online privacy attitudes and behaviours (Bartel-Sheehan, 1999; Fogel & Nehmad, 2009; Kehoe et al., 1997; O'Neil, 2001; Westin, 1997; Youn & Hall, 2008). When compared to males, females perceived greater privacy risks when online, reported higher levels of privacy concern, were more concerned about instituting laws aimed at protecting privacy online, were more likely to review and control available privacy settings online and were more likely to provide aliases on web-pages (Kehoe et al., 1997; O'Neil, 2001; Youn & Hall, 2008). Recent research by Grubbs-Hoy and Milne (2010) found that females engaged in various privacy protection behaviours more often than males, including greater discretion when posting and un-tagging photos, accepting friends and joining groups. Gender differences also seem to be important in understanding who is and who is not likely to read privacy policies. Milne and Culnan (2004) found that men were less likely than women to read privacy policies. Based on previous research, it was anticipated that females would report higher levels of online privacy concern, as well as report exhibiting a greater number of behaviours geared toward protecting online personal privacy. Moreover, it was expected that females would be more likely to employ privacy settings than their male counterparts.

The "Virtual Other"

"People's willingness to share depends on who they are sharing the information with" (Olson, Grudin & Horvitz, 2005, p. 1987). Presumably, in the case of online profiles and personal web-pages, users have a receiver in mind when constructing or deciding to share personal details. While this 'other' is not an interactive partner per se, that is, they do not respond directly to the profile creator, they are nonetheless an end goal or target. It is suggested that the virtual other may best be characterized as a psychological other, or a mental representation of an audience. For example, a young woman posts her best pictures on her online profile, and highlights all of her best qualities in hopes that an old flame might come across her profile and see how she has progressed since their break-up. Alternatively, a young woman might choose not to post certain personal details (e.g., pictures of her drunk at a party or in compromising poses at a nightclub) due to the fear that a relative, co-worker or even stranger might see her profile and form negative judgments about her person based on the information presented. Decisions about how much and what types of information to share may very well be dependent on who the user is thinking about at the time. At present there is no literature addressing the "virtual other" in an online setting. The current research provides a first exploratory investigation of the target "other".

Impact of Media (Context)

The context in which information is shared has an impact on levels of disclosure (Joinson, 2001; Schouten, Valkenburg & Peter, 2007; Wood, Nosko, Desmarais, Ross & Irvine, 2006). The general consensus is that online media, when compared to more

traditional media such as paper-and-pencil, over the telephone, and face-to-face, tend to encourage higher levels of disclosure (Joinson, 2001; Locke & Gilbert, 1995; Tidwell & Walther, 2002; Wood, Nosko, Desmarais, Ross & Irvine, 2006). Research has proposed the presence of the online disinhibition effect (Suler, 2004), whereby various features of the online context (e.g., anonymity, invisibility, and asynchronicity of communication) may help to explain why patterns of disclosure differ online and offline. Specifically, as a result of the perceived psychological distance fostered by anonymity offered online, users are more relaxed, are more likely to "open up" and may even feel less restrained (Suler, 2004), thus resulting in greater disclosure. In the present study, the impact of media on users' decisions to share information in personal profiles was examined. It was anticipated that the online condition, as compared to disclosure on paper-and-pencil, would generate higher levels of disclosure. No known studies exist comparing the impact of media on privacy setting use in personal profiles, therefore this aspect of the investigation was exploratory in nature.

Summary of the Present Study

The purpose of Study 2 was to further explore the factors that may influence the choice to self-disclose various types of information online in Facebook profiles and the choice to employ privacy settings. The three main lines of inquiry outlined above were addressed as follows. First, this study addressed the impact of type of story read prior to constructing a profile. Specifically, two groups were exposed to privacy relevant information prior to constructing a Facebook account. One group read an anecdotal story depicting the case of a young woman who was stalked and found as a result of the

information she had posted about herself on her Facebook account. A second group was required to read a more formal review of privacy policies that is found on the Facebook website. These two groups were compared to one another and to a third group who read a story that simply reviewed the history of the Internet. It was expected that participants who read a salient personal privacy invasion story (Personal Privacy Story) would be the least inclined to disclose information online, and the most inclined to set privacy settings, as compared to those reading either the Facebook privacy policy (Legal Privacy Agreement Story), or a story about the history of the Internet (History of the Internet Control Story).

The second issue sought to address additional variables that might also have an impact on the decision to disclose information or use privacy settings. Given previous research identifying gender as a key concern, target person gender (i.e., whether the profile participants created was for a male or female), and the gender of the participant (male, female) were also considered. In order to ensure a degree of control and consistency over the information that was included in the profiles, participants were asked to create profiles based on information for a target person. Information provided to participants in the study was consistent across participants with the exception of the target person's gender (some received information about a female target and others received information about a male target) and photos of the target individual[4].

[4] Independent raters (4 females, 3 males) evaluated the photos based on three criteria. attractiveness, sociability and friendliness. Results indicated that ratings were similar for both sets of photos.

It was expected that female participants would reveal less and employ more privacy settings overall. It was also expected that the story type might impact on the amount of information disclosed and the number of settings employed such that female participants exposed to the anecdotal story would disclose the least amount of information and employ the most privacy settings as this story in particular depicts the particular risks for women on social networking profiles.

Further, this study sought to examine from an exploratory perspective which factors such as demographic variables (age and relationship status), personality (e.g., extraversion, self-consciousness), computer usage (e.g., familiarity with computers, Facebook usage), reported privacy attitudes and behaviours, the virtual "other" (who it is the user is thinking about when posting information) and self-report levels of disclosure predicted actual disclosure and privacy settings use in Facebook profiles.

Finally, the third issue examined the impact of media with a contrast between online and hard copy (paper-and-pencil) formats for filling out a personal profile. The role of media was examined within the context of the other variables identified above. Specifically, the study sought to examine the impact of target gender (i.e., whether the profile participants created was for a male or female), gender of the participant (male, female) and type of media used (paper-and-pencil, online in Facebook) for generating profiles on information that was disclosed and the likelihood to employ privacy settings. Based on online hyper-personal theory (Walther, 1996) and previous research showing that online media generated higher levels of disclosure (Joinson, 2001; Schouten, Valkenburg & Peter, 2007, Wood, Nosko, Desmarais, Ross & Irvine, 2006), it was

expected that participants filling out a profile on paper-and-pencil would be less inclined than their online counterparts to disclose information. No specific hypotheses were set forth for privacy settings usage as a function of media context. There is no known research examining the impact of context on settings use, and therefore this examination was exploratory in nature.

Summary of Hypotheses

1. The Personal Privacy Story would result in the least disclosure of information and the most use of privacy settings among the three story types.

2. The Legal Privacy Agreement Story would result in less disclosure of information and use of more privacy settings than the Internet History Story.

3. If consistent with face-to-face interactions, female participants would disclose more overall information online, but employ more privacy settings than male participants.

4. There would be less disclosure and greater use of privacy settings for female targets than male targets.

5. There would be an interaction such that females would employ more privacy settings and disclose the least amount of information for female targets in the Personal Privacy Story.

6. Explorations of variables including the virtual other, personality and experience issues were exploratory and no specific hypotheses were derived.

7. There would be more disclosure of information in the online media condition than in the paper and pencil media condition. The impact of this manipulation on

privacy setting use was exploratory. The impact of gender was also exploratory in this analysis.

General Method

Participants. In total, 236 first-year undergraduate psychology students enrolled in an Introductory Psychology course at Wilfrid Laurier University participated. Participants were recruited through a voluntary sign-up system and were given 2% in compensation towards their introductory psychology course grade. Participants included 100 male participants and 136 female participants, with ages ranging from 17 to 27 years (X_{age} = 18.55, SD = 1.16). Independent t-tests revealed that gender differed significantly by age (t (234) = 2.21, p = .03), with males being slightly older than females ($M_{agemale}$ = 18.74 years, $M_{agefemale}$ = 18.40 years). Although significant statistically, this was not considered a meaningful difference given that the mean age of both groups was 18 years of age. Approximately 65% of the sample reported currently being in a romantic relationship, 34% reported being single, and the remaining 1% were either married or engaged. Two-hundred and twenty seven participants indicated that they currently had a Facebook account. All participants were treated in accordance with APA ethical guidelines.

Participants were randomly assigned to one of 3 groups: one of three story conditions, either the female or male target for the profile construction and either the online or paper-and-pencil media context. Specifically, among the story conditions participants were randomly assigned to one of three story conditions: History of the Internet Control Story (N = 78), Legal Privacy Agreement Story (N = 77) and Personal

Privacy Story (N = 81), and one of two target conditions: Michael (N = 102) and Sarah (N = 134). (See Tables 8 and 9 for breakdowns of story condition by gender of the target male and female participants, respectively). For the media context evaluation, participants were randomly assigned to one of two methodology conditions: paper-and-pencil (N = 129) or online (N = 107), and one of two target conditions: Michael (N = 102) and Sarah (N = 134). (See Tables 10 and 11 for a breakdown of context condition by participant gender for male and female participants, respectively).

Materials

Several sets of materials were constructed for this study, including stories, target person portfolios, Facebook accounts, paper-and-pencil hard copy materials matching the online condition, privacy settings booklets and some measures for the survey. Other materials were drawn from existing research including survey scales and scoring schemes. These materials are outlined below.

Stories. There were three stories: History of the Internet Control Story, the Legal Privacy Agreement Story and the Personal Privacy Story (See Appendix C). All three stories were constructed to be approximately equal in length (506, 496, and 496 words, for the control, legal and personal story, respectively). Participants read one of three stories. In two conditions the stories provided information regarding privacy. In the History of the Internet Control Story condition, participants read a short passage that described the history of the Internet and its popularity. This vignette did not discuss privacy issues. The Legal Privacy Agreement Story was an excerpt taken directly from the privacy statement on the Facebook online website. This excerpt discussed the legal

privacy terms associated with the online network. The Personal Privacy Story was an adaptation of a story that appeared in the Globe and Mail (September 2008) which outlined potential consequences of putting personal information online. This vignette described the story of a young woman who was stalked and later approached by a reporter in a local coffee shop. The reporter went on to explain that he had located her by using only the information she had posted in her Facebook profile. She was shocked to find out that a complete stranger was able locate her actual whereabouts and identify her personally, without her awareness.

Facebook Target Person Portfolio. Participants used information from a pre-made portfolio that included the personal information of two fictional individuals: Sarah Barnes and Michael Barnes (see Appendix D). Information included a personal resume, an employment application, a list of the individual's "25 things about me", a short "About me" summary and a series of photos. Various pieces of information were included in the booklets that represented default, sensitive and stigmatizing information, as well as information relevant to various topics, such as relationship information and work information. For example, sexual orientation, religious and political views were included in the portfolio, and were considered stigmatizing information. All information was identical in the two pre-made portfolios (e.g., both Sarah and Michael were 25 years old, both had the same degree from the same university, the same work history etc.), with the exception of photos and names. Participants used the information in the portfolios to create a Facebook profile.

Materials for the Online Condition

For the online condition, participants were provided with a folder on the desktop that contained all of the photos that were in the portfolio, so that they could upload the photos directly into Facebook. While photos for Michael and Sarah depicted a different person, there photos that were chosen were equivalent in content. For both, photos were goofy, serious, and contained shots of scenery, friends, family and relationship partners. Participants were tested individually, using the same make and model of PC based computers with Internet access. All participants used the standard Facebook website to construct their profile.

Facebook Accounts. Online Facebook accounts were generated for each participant in the online condition. Prior to the study session, researchers created a series of new email accounts in Hotmail which were then used to open up associated Facebook accounts. Each Facebook account was opened using the newly created email address, a fictitious name, and fictitious birth date information. The existing blank Facebook accounts were then used during the study session. Participants were able to upload any photos and include any information in their profile that they desired, based on the information provided to them in the pre-made target portfolio.

Materials for the Paper-and-Pencil Condition

Participants in the paper-and-pencil condition were provided with a paper-and-pencil version of a Facebook profile (see Appendix E for an example page). This 27 page booklet consisted of one screenshot of each page available to users online when actually in Facebook, including the pages that outlined privacy setting options. All of the available drop down tab options and checkbox options were displayed in the screenshots

so that participants could simply circle their preferred choice. Participants were also provided with a series of 13 numbered photos printed on paper that they could choose to include in their profile. These photos were identical to the photos included in the online condition. They simply indicated by photo number which one they wished to include in albums or as a profile picture. Participants could include any information in their profile that they desired, based on the information provided to them in the pre-made target portfolio.

Privacy Settings Booklet. Participants were provided with a privacy settings booklet that outlined all of the privacy and account settings available to users in Facebook (see Appendix F for an example page from the privacy settings booklet). The eight page booklet contained subheadings with specific types of settings that participants could easily flip to for reference. All settings were described, and then screenshots of the actual settings page as seen online were provided. In addition, instructions on how to employ each setting were provided. For example, participants were provided with statements such as "If you want to limit or control who can search for you on Facebook, you can click on "search visibility", and choose from a variety of settings (e.g., only friends can search for you, all my networks and friends of friends, so virtually anyone). You can also limit what people can see about you, and how they can contact you after locating your profile online".

Scoring tool. This study used an existing scoring tool that was established for coding Facebook profiles (see Study 1 A, B and C). This scoring tool allowed for assessment of overall disclosure in Facebook (based on coding scheme from Study 1 A),

disclosure across three categories of information (personal identity information, sensitive personal information, and stigmatizing information) (based on coding scheme from Study 1 B), disclosure within various topic areas (e.g., personal information, work information) (based on coding scheme from Study 1 C), and employment of privacy settings within Facebook. The pre-established checklist was comprised of 97 dichotomously scored items (i.e., whether the piece of information was present or absent) and three identification items (i.e., username link, the network searched, and the size of the overall network). To examine disclosure of content within Facebook, eight of the topic categories from Study 1 C were adopted for the current study, including: Personal information, Picture and Album information, Work information, Education information, Age information, Contact information, View information, and Relationship information. These eight were chosen based on the information that participants could include in the profiles. For example, some of the scales used in Study 1 C contained items that were not provided to users, and were thus not included in the profiles.

To assess use of privacy settings, an additional 25 dichotomously scored items were added to the scoring tool. Each of the 25 new items represented a possible change in privacy settings. A three step process was used to establish the privacy settings coding scheme. First, a blank Facebook profile was created. Second, a researcher signed into the blank profile and recorded all of the pre-set or default privacy settings. Third, for all of the participant profiles, settings were recorded, and for each privacy setting that was changed from the default setting, a score of 1 was given, if no change was made, a score of 0 was given. For example, users are able to change the "public search" option, or

whether or not other users in Facebook can search for them through Facebook by means of typing their name into a search bar. By default, this option is selected, allowing for public search. In this case, this setting, if selected, would receive a score of 0 indicating that no change was made from the default. Alternatively, if unchecked or unselected, a score of 1 would be assigned indicating that a change had been made to the setting.

Online Survey. Participants completed an online survey at the beginning of the study session (see Appendix G). This survey contained a broad range of measures, including standardized and newly created measures. The first section included a demographic sheet. The second section contained measures assessing perceptions of technology, uses of technology and Facebook and familiarity with technology. The third section assessed views about the self (i.e. self-disclosure and public self-consciousness), personality (extraversion), and privacy attitudes and behaviours (e.g., privacy behaviours when online, concern for privacy in general and online). Lastly, participants responded to a scale assessing perceptions of the virtual other (the audience for whom they are disclosing), and a measure of social desirability.

Demographics. Participants responded to three questions pertaining to age, gender and relationship status.

Unstandardized/Newly Created Measures.

For descriptive information for unstandardized/newly created measures and items, refer to Tables 12 and 13. The following scales were chosen based on previous research that has examined factors related to use of technology (e.g., Amichai-Hamburger, Wainapel & Fox, 2002; Buchanan, Paine, Joinson & Reips, 2007; Butt & Phillips, 2008; Mueller,

Wood, Willoughby, Ross & Specht, 2008) and the need to explore potentially novel predictors of use such as the virtual audience.

Computer Use. Participants were asked to indicate how many hours per week they used the computer for three purposes, including: the internet, recreation (e.g., games, communication), and work/school. Participants were asked to fill in the number of hours per week they used the internet for each purpose.

Attitudes towards Computers (Mueller, Wood, Willoughby, Ross, & Specht, 2008). This measure assessed general computer use and expertise (familiarity with computers) as well as comfort and ease with computers and the Internet. In total, there were three items in this scale. For example, participants were asked how knowledgeable they were about using computer software. Response options ranged from 1 (very knowledgeable) to 7 (not at all knowledgeable). Participants were also asked about how comfortable they felt when using computers. Response options ranged from 1 (very comfortable) to 7 (very uncomfortable). Cronbach's alpha was .80, indicating good reliability.

Internet Security Concerns and Behaviours. This measure contained 26 items assessing concern with internet security, as well as behaviours related to protecting security online. This measure employs 7-point Likert type scales, with response options ranging from 1 *(not at all true of me)* to 7 *(absolutely true of me)*. Participants were asked to respond to statements such as "Please indicate the degree to which you have used this strategy to protect your privacy online: Installed Antivirus software". Cronbach's alphas for the concern subscale were .87 and .91 for Virus Concern and Entity Concern,

respectively, indicating high reliability. For the Strategy Use Subscale, Cronbach's alphas were .75 for Software Strategy Use, .60 for and Privacy Strategy Use, and .44 for Password Strategy Use, indicating low to moderate high reliability.

Facebook Usage Scale. Various items from Viégas' (2005) Blog Survey were adopted and modified, and new items were created and added to this scale. The Facebook Usage Scale assessed types of information posted on Facebook, amount of time spent using Facebook, awareness of other users' Facebook behavior, and familiarity and use of privacy settings in Facebook. In total, this measure contained 13 items and employed 5-point Likert type scales. For the two subscales Degree of Disclosure and Consideration of Disclosure, Cronbach's alphas were .65 and .47, respectively, indicating moderate to low reliability.

Facebook Privacy Settings Behaviours. Participants were asked about their privacy settings behaviours when using Facebook. For example, participants were asked to respond to items such as "How familiar are you with Facebook privacy settings?", and "How often have you advised others to employ their privacy settings?" In total, this measure contained 3 items, and employed 7-point Likert type scales. Cronbach's alpha for this measure was .79.

The Virtual "Other". Participants were asked to indicate who they were thinking of (the audience) when posting personally revealing information. Participants were asked the following statement, "When you post personally revealing information in your profile, who are you thinking about?" Response options included: No one in particular, friends, family, business associates, employer, romantic partners, instructors,

acquaintances, ex-romantic partners, strangers, and anyone, and were rated using a 1 *(not at all true of me)* to 7 *(absolutely true of me)* Likert type scale. Participants were also asked to indicate with a "yes" or "no" whether or not there was someone or something limiting them from posting information. The two items in the Myself/Friends subscale were significantly correlated at the .001 level (r = .57). Cronbach's alpha for the Other Referents subscale was .83, indicating good reliability.

Short Privacy Survey. Participants responded to items assessing their use of the privacy booklet provided to them in the study. In addition, participants indicated on a scale from 1 *(not at all enjoyable)* to 7 *(extremely enjoyable)* how enjoyable they found the profile creation task. In total, this measure contained 6 items, and employed a variety of question types including 7-point Likert type scales, dichotomous yes or no response options, and fill-in-the-blanks.

Standardized Measures

For descriptive information for each standardized measure and corresponding subscale refer to Table 14.

Self-Disclosure: The Temperament and Target Inventory (Cloninger, Przybeck, Svrakic & Wetzel, 1994). This measure consisted of 13 items assessing self-disclosive behaviours, and employed a 7-point Likert scale. Participants were asked to respond to statements such as "I am open about my feelings", with response options ranging from 1 (*not at all true of me*) to 7 (*very true of me*). Higher scores indicated higher levels of self-disclosure. Previously established reliability for this scale was .86.

A Cronbach alpha for the overall measure was calculated for the present sample with an outcome of .91, indicating very good reliability.

Personal Attributes Survey (PAS): Public and Private Self-Consciousness (Buss, 1980). This measure consisted of 22 items assessing both public and private self-consciousness, and employed a 7-point Likert scale with response options ranging from 1 (*not at all true of me*) to 7 (*very true of me*). This scale consisted of two subscales, public and private self-consciousness. A total score of 12 was possible for the public self-consciousness subscale, and a total score of 10 was possible for the private self-consciousness scale. A higher score on each subscale indicated higher levels of these factors. Participants were asked to respond to statements such as "I worry about what people think of me", and "I spend time reflecting on things". Previously established reliabilities for the subscales were .77 (Public SC) and .81 (Private SC). A Cronbach alpha for the overall measure was calculated for the present sample with an outcome of .89, indicating good reliability. Reliability was also calculated for each of the individual subscales, revealing alphas of .85 for the public self-consciousness subscale and .87 for the private self-consciousness subscale, indicating higher reliability than reported in previous assessments.

The Balanced Inventory of Desirable Responding (BIDR) version 6 – Form 40A (Paulhus, 1984). This measure consisted of 40 items assessing social desirability tendencies and employed a 7-point Likert scale. The BIDR consisted of two subscales, impression management (IM) and self-deceptive enhancement (SDE). A total score of 20 was possible for each subscale, with a possible overall score of 40 for the entire

measure. Higher scores indicated more socially desirable responses. Participants were asked to respond to statements such as "I always know why I like things", with response options ranging from 1 (*not true*) to 7 (*very true*). Reliabilities for the subscales were .77-.85 (IM) and .67-.77 (SDE) based on a sample of undergraduates from the University of British Columbia. A Cronbach alpha for the overall measure was calculated for the present sample with an outcome of .77, indicating similar reliability as reported in previous assessments. Reliability was also calculated for each of the individual subscales, revealing alphas of .71 for the IM subscale and .69 for the SDE subscale.

BIG FIVE: short version (TIPI) (Gosling, Rentfrow & Swann, 2003). This measure consisted of 10 items assessing personality and employed a 7-point Likert scale with response options ranging from 1 (*Disagree strongly*) to 7 (*Agree strongly*). The TIPI consisted of 5 subscales with 2 items in each including: Extraversion, Agreeableness, Conscientiousness, Emotional Stability, and Openness to Experiences. Participants were asked to indicate the extent to which they agreed or disagreed with statements such as, "I see myself as: _____ Extraverted, enthusiastic". A higher score on each subscale indicated a tendency towards that particular personality trait. Correlations between each of the five pairs of items were significant, suggesting good reliability (.47, .15, .30, .51, and .27, for Extraversion, Agreeableness, Conscientiousness, Emotional Stability, and Openness to Experiences, respectively). The TIPI is recommended for use in studies that contain multiple surveys and in cases where time is a constraint, such as in the case of the current study where a large number

of measures were used. In addition, according to Gosling and colleagues, when compared to the larger Big Five measure of personality the TIPI yielded adequate levels of convergence with widely used Big Five measures, test-re-test reliability, and convergence between self and others ratings. For these reasons, the decision was made to use the shorter version.

Online Privacy Attitudes Scale (Buchanan, Paine, Joinson & Reips, 2007). This measure consisted of 16 items assessing concerns about establishing and maintaining privacy online. This scale employed a 7-point Likert scale ranging from 1 (*not at all concerned*) to 7 (*very concerned*). Participants are asked to respond to statements such as "In general, how concerned are you about your privacy while you are using the internet?" Higher scores indicated a greater concern for maintaining privacy online. A Cronbach alpha for the overall measure was calculated for the present sample with an outcome of .93 indicating very high reliability.

Online Privacy Behaviours Scale (Buchanan, Paine, Joinson & Reips, 2007). This measure consisted of 12 items assessing behaviours related to establishing and maintaining privacy online. This scale employed a 7-point Likert scale ranging from 1 (*not at all concerned*) to 7 (*very concerned*). Participants are asked to respond to statements such as "How often do you watch for ways to control what people send you online (such as check boxes that allow you to opt-in or opt-out of certain offers)?" This measure consisted of two subscales: General Caution (N= 6) and Technical Protection (N= 6). Higher scores indicated higher levels of privacy behaviours related to these factors. A Cronbach alpha for the overall measure was calculated for the present sample

with an outcome of .80 indicating high reliability. Reliability was also calculated for each of the individual subscales, revealing alphas of .78 for the General Caution subscale and .72 for the Technical Protection subscale.

Procedure

Prior to participating, all participants completed a consent form (see Appendix H).

Upon consent, participants were instructed to complete the online survey at the beginning of the study session. All participants filled out the online survey on individual computer terminals. In order to ensure privacy of response, participants were seated at every other computer terminal, allowing ample space in between participants. Sessions ranged from one to 15 participants with five participants being tested at once on average, which enhanced compliance and ensured that participants read the stories provided to them. Following the completion of the online survey task, participants were given one of the three privacy stories to read. After reading the story, participants in the online condition were given Facebook log-in information, including an individual user name and password. Once participants were logged into a blank Facebook profile, they were told to construct an online personal profile for the person whose information they had been given (Michael or Sarah). In the paper-and-pencil condition, participants were provided with a booklet of screenshots that directly corresponded to each screen viewable in Facebook and they were told to construct an online personal profile for the person whose information they had been given (Michael or Sarah). For the cover story, participants were told that there were two conditions, one in which they created a profile

for themselves and another where they created a profile for another person. They were told that they were assigned to the condition where they would create a profile for someone else based on that person's actual information. In order to encourage participants to complete the profiles in as natural a way as possible, all participants were told in the cover story that the target person for whom they were creating the profile was a real person, that they had volunteered their personal information, and that this person may have the opportunity to view the profile once it was completed. All participants were instructed to use as much or as little information as they felt necessary. A verbal explanation of the constraints of the study was expressed to each participant, including the inability to add friends, join a network, or upload applications. In order to obtain as much information as possible about which pieces of information users would have liked to include in the profile, participants were instructed to indicate on the profile wall any additional information or features that they would have wanted included in the profile, but were not able to include (e.g., join a network, add friends etc.). In addition, all participants were provided with a booklet containing information about all of the available privacy settings in Facebook. Each participant was told that if they wished they could find detailed instructions describing the privacy settings on Facebook within the privacy settings booklet. Once they finished developing the online profile, participants were given the short 7-item survey. The sessions took approximately an hour and 15 minutes to complete. Finally, after completing the study each participant received a debriefing form describing important privacy information, along with a summary of the current study (see Appendix I). Upon completion of the study session, a trained

researcher came in and coded each Facebook profile for overall content and privacy settings.

Results

Given the number of analyses and the different focal points in the present study the results are divided into sections to more clearly depict the analyses specific for each focal point of the study. Three sections are provided; Effect of Story and Gender, Additional Exploratory Predictors, and Effect of Media and Gender[5].

Question 1

Effect of Story and Gender. The first area of inquiry involved examination of the impact of the stories on the construction of Facebook accounts.

Design

To address the first line of inquiry, a 3 (Story condition: Personal Privacy Story, Legal Privacy Agreement Story, History of the Internet Control Story) x 2 (Participant gender: Male, Female) x 2 (Target gender: Male, Female) experimental design was employed.

Analyses

Analyses explored whether any differences in disclosure and use of privacy settings in Facebook emerged as a function of story condition, gender of target and

[5] Cell sizes were insufficient to analyze story, context and gender together. Therefore, the decision was made to analyze the effects of story and gender and context and gender separately.

gender of participant[6]. Examination of these variables was carried out using univariate and multivariate analyses of variance (MANOVA). Three analyses were conducted to examine disclosure: one for overall disclosure, one for disclosure divided into three grouping categories (Personal identity information, Sensitive personal information, and Stigmatizing information), and one for disclosure within eight content areas with Facebook (Personal information, Picture and Album information, Work information, Education information, Age information, Contact information, View information, and Relationship information)[7]. Privacy settings were examined using regression analyses. It is important to note that only 49 participants out of 236 changed at least one privacy setting.

Overall Disclosure. A univariate analysis of variance was conducted to examine overall disclosure within the Facebook profiles. Story condition, gender of target and gender of participant were entered as the fixed factors, and overall disclosure was entered as the dependent variable. Results revealed that there were no significant main effects of any of the fixed factors (largest $F = 1.38$) (See Table 16).

Disclosure of Personal Identity Information, Sensitive Personal Information, and Stigmatizing Information. To address the question of how much information

[6] In order to examine disclosure as a function of privacy settings usage, all analyses examining story and gender were repeated using only those participants who did not employ settings. Patterns were consistent with results found for the entire sample.

[7] Coding categories were adopted from Study 1 B and 1 C (see Scoring Tool in Materials section).

participants disclosed in three risk categories (Personal identity information, Sensitive personal information, and Stigmatizing information), a multivariate analysis of variance was conducted. For disclosure in the three grouping categories, story condition, gender of target and gender of participant were entered as the fixed factors, and personal identity information, sensitive personal information, and stigmatizing information were entered as the dependent variables. Results revealed that although there were no significant main effects, there were two significant interactions.

First, there was a significant interaction of gender of participant and story condition for sensitive information (See Table 17). Two follow-up one-way ANOVAs were conducted, one for males and one for females, to identify where the differences were occurring. For each, story condition was entered as the between subjects variable, and sensitive information was entered as the dependent variable. Results revealed that the difference was significant for females (F (2, 130) = 3.36, p = .04), such that they disclosed significantly more sensitive information in the History of the Internet Control Story condition, and significantly less sensitive information in the Legal Privacy Agreement Story condition (See Table 17).

Second, there was a significant interaction of gender of participant and gender of target for stigmatizing information (See Table 17). Two follow-up one-way ANOVAs were conducted, one for male targets and one for female targets, to identify where the differences were occurring. For each, gender of the participant was entered as the between subjects variable, and stigmatizing information was entered as the dependent variable. Results revealed that the difference was significant for female targets (t (129) =

2.36, $p = .02$), such that male participants disclosed more stigmatizing information for a female target than did female participants (See Table 17).

Disclosure within Facebook Content Areas. To address the question of how much information participants disclosed in eight content areas within Facebook (Personal information, Picture and Album information, Work information, Education information, Age information, Contact information, View information, and Relationship information), a multivariate analysis of variance (MANOVA) was conducted. Story condition, gender of target and gender of participant were entered as the fixed factors, and all eight topics were entered as the dependent variables.

Results revealed that there was a significant main effect of gender of participant for one out of the eight topics. Specifically, when disclosing contact information in particular, males included significantly more than did females (See Table 18). While there were no significant main effects for either story condition or gender of the target, the main effect was qualified by significant interactions.

Specifically, results revealed four significant interaction effects, two for contact information and two for view information. First, there was a significant interaction of gender of participant and story condition for contact information (See Table 18). Two follow-up one-way ANOVAs were conducted, one for males and one for females, to identify where the differences were occurring. For each, story condition was entered as the between subjects variables, and contact information was entered as the dependent variable. Results revealed that the difference was significant for males, (F (2, 97) = 3.24, $p = .04$), such that they disclosed significantly less contact information in the History of

the Internet Control Story condition than either of the Legal Privacy Agreement Story or Personal Privacy Story conditions (See Table 18). Interestingly, while story condition did not have a significant impact on disclosure for female participants, it is of note that females disclosed less overall than males in both the Legal Privacy Agreement Story and Personal Privacy Story conditions.

Second, there was a significant interaction of story condition and gender of the target for contact information. Three follow-up independent t-tests were conducted, one for each story condition, to identify where the differences were occurring. For each, gender of the target was entered as the grouping variable, and contact information was entered as the dependent variable. Results revealed that after having read the personal privacy story, there was less disclosure of contact information for female targets than for male targets (See Table 18).

Finally, there were significant interactions of gender of participant and gender of target for both contact and view information. For contact information, two follow-up independent t- tests were conducted, one for males and one for females, to identify where the differences were occurring. For each, gender of target was entered as the grouping variable, and contact information was entered as the dependent variable. Results revealed that the difference was significant for males, ($t(98) = 2.55, p = .01$), such that they disclosed significantly more contact information for male targets than they did for female targets (See Table 18). For view information, a follow-up independent t- test was conducted, one for male targets and one for female targets, to identify where the differences were occurring. For each, gender of participant was

entered as the grouping variable, and view information was entered as the dependent variable. Results revealed that the difference was significant for female targets, ($t(130) = 2.70$, $p = .008$), such that male participants disclosed far more view information about a female target than did female participants (See Table 18).

Privacy Settings Use. While only 48 participants out of 236 (20.3%) changed at least one privacy setting, this was not unexpected. Previous research has found that very few users choose to employ privacy settings (e.g., Berendt, Gunther, & Spiekermann, 2005; Gross & Acquisti, 2006; Milne & Culnan, 2004). Preliminary analyses indicated that each condition had at least one participant who employed privacy settings. Due to small sample sizes, only descriptive analyses were available[8]. A count was conducted to compare privacy settings by story condition, and revealed that more privacy settings were employed in the Personal Privacy Story condition as compared to the two other story conditions. In terms of gender of the participant, females tended to employ more settings than did males. For target gender, males and females employed more settings for a target of the same gender. Finally, females in the Personal Privacy Story condition employed more settings for female targets in particular (See Table 19).

Question 2

Additional Exploratory Predictors. The second area of inquiry involved an exploratory examination of additional variables that may predict disclosure and privacy settings use.

[8] Non-parametric analyses were not possible given that 71.4% of expected cell sizes that were less than 5.

Factor analysis: Scale aggregation

In order to firmly establish which items should be aggregated, to confirm the relationships between these variables, and to identify the factors underlying the data, a principal components factor analysis with a Varimax rotation was conducted for four out of the eight created measures used in the current study. Only those items within each measure that were assessed using the same scale (e.g., 7-point Likert type scale) were included in the factor analyses.

Items were selected based on two criteria. First, factors were selected that were measured by more than one item. Second, items that loaded highly on one factor were retained. Items that loaded moderately on more than one factor were judged not only based on factor loadings, but on item content and theory. The decision was then made to group these particular items together with items of a similar nature. Reliability was conducted for scales that had more than 3 items using Cronbach's alpha.

Attitudes towards Computers. For the attitudes towards computer scale, three items were subjected to factor analysis, and results revealed that there was one factor with an Eigenvalue greater than 1.00 (Eigenvalue = 2.48), which accounted for a total of 82.60% of the variance. The factor loading matrix is presented in Table 19. The following aggregate scale was created based on the factor loadings: *Positive Attitudes towards Computers*. Cronbach's alpha was .80, indicating good reliability.

Internet Security Concerns and Behaviours.

Concern Subscale. There were two factors with Eigenvalues greater than 1.00, which collectively accounted for a total of 76.95% of the variance. Eigenvalues ranged

were 1.04 and 5.12, and indicated that the two factors explained 12.98% and 63.98% of the variance, respectively. The factor loading matrix is presented in Table 20. Two aggregate scales were created based on the factor loadings: *Virus Concern* and *Entity Concern. Virus concern* referred to a concern over breaches in security from virus, spam and spyware. *Entity concern* referred to a concern over breaches in online security from hackers, online stalkers and other unauthorized access by a party or individual. Cronbach's alpha was .87 for *Virus Concern* and .91 for and *Entity Concern*, indicating high reliability.

Strategy Use Subscale. There were three factors with Eigenvalues greater than 1.00, which collectively accounted for a total of 60.03% of the variance. Eigenvalues ranged from 1.17 to 2.82, and indicated that the three factors explained 12.97%, 15.78 and 31.28% of the variance, respectively. The factor loading matrix is presented in Table 21. Three aggregate scales were created based on the factor loadings: *Software Strategy Use, Privacy Strategy Use* and *Password Strategy Use*. Cronbach's alphas were .75 for *Software Strategy Use*, .60 for and *Privacy Strategy Use*, and .44 for *Password Strategy Use*, indicating low to moderate high reliability.

Facebook Usage Scale. For the Facebook usage scale, there were five factors with Eigenvalues greater than 1.00, which collectively accounted for a total of 58.07% of the variance. Eigenvalues ranged from 1.02 to 2.50, and indicated that the five factors explained 19.25%, 13.00%, 9.74%, 8.27% and 7.81 % of the variance, respectively. The factor loading matrix is presented in Table 22. Results indicated that no items loaded highly on the fourth factor (highest loading = .40), therefore this factor was omitted.

Two items, "How well do you feel you know your profile's audience?" and "How liable do you think you are for the things you post in your profile?" were the only items to load on factors three and five, respectively, and were therefore omitted from scale aggregation. The following two aggregate scales were created based on the factor loadings: *Degree of Disclosure* and *Consideration of Degree of Disclosure*. Cronbach's alpha was .65 for *Degree of Disclosure* and .47 for and *Consideration of Degree of Disclosure*, indicating low to moderate reliability.

Facebook Privacy Settings Behaviours Scale. For the Facebook Privacy Settings Behaviours Scale there was one factor with an Eigenvalue greater than 1.00, which accounted for a total of 70.58% of the variance. The Eigenvalue was 2.12, and indicated that the factor explained 70.58% of the variance. The factor loading matrix is presented in Table 23. The following aggregate scale was created based on the factor loadings: *Privacy Settings Behaviour*. Cronbach's alpha was .79.

The Virtual Other. For the Virtual Other, there were four factors with Eigenvalues greater than 1.00, which collectively accounted for a total of 68.49% of the variance. Eigenvalues ranged from 1.00 to 4.24, and indicated that the four factors explained 35.31%, 15.37%, 9.44% and 8.37 % of the variance, respectively. The factor loading matrix is presented in Table 24. No items loaded highly on factor three (highest loading = .33), so this factor was omitted. One item, "When you post personally revealing information in your profile, who are you thinking about? No one", was the only item to load highly on factor four and was therefore omitted from scale aggregation. The following two aggregate scales were created based on the factor

loadings: *Myself/Friends* and *Other Referents*. The two items in the *Myself/Friends* subscale were significantly correlated at the .001 level ($r = .57$). Cronbach's alpha for *Other Referents* was .83, indicating good reliability.

Design

The design of the current study included a number of variables that could identify what factors predict disclosure of information in terms of personal attitudes, experiences and behaviours and also variables that could potentially explain disclosure apart from the experimental manipulations. Analyses of these variables were exploratory as their impact was not directly associated with previous literature. Specifically, a series of regressions were conducted to examine the predictive power of various variables including attitudes towards computers, online privacy attitudes, online privacy behaviours, personality, social desirability, reported disclosure and the virtual other. Scales that measured similar constructs were examined together in the analyses. For example, all the personality measures were examined as potential predictors in one regression. This was done to increase parsimony in the analyses, and to examine the predictive power of specific categories of variables (e.g., personality, online privacy attitudes) that may have been associated with disclosure and use of privacy settings. In total, there were seven groups of predictor variables. For an overview of the measures within each of the seven groups, refer to Table 25.

Descriptives

For the short privacy survey, 25.3% of participants reported using the privacy setting booklet that was provided (65% did not use it, and 9.7% did not answer this

question). When asked why they did not use the booklet, of those who gave a response, 40.1% participants indicated that they already knew the settings, .8% indicated they had no time to read it, 3.5% were not interested in reading it, 3.1% didn't want to use the booklet, and 2.7% were not interested in using privacy settings. The remaining 15.6% indicated a combination of reasons for not using the booklet including lack of interest, already knowing about the settings and lack of time to read through the booklet. Of the 25.3% of participants who did use the booklet, 44.6% reported that they learned something new about the privacy settings (49.2% indicated they did not learn anything new, and 6.2% did not answer this question). When asked about how enjoyable the task was of creating a Facebook profile for another person, the majority of participants indicated that they found the task to be more than somewhat enjoyable (i.e., indicated 5 on a 7-point scale ranging from 1 (not at all enjoyable), to 7 (extremely enjoyable). Participants were also given the opportunity to fill in a comment box about the study. A common theme emerged, whereby participants commented on how it really made them think twice about what they were including in the profiles, especially because the information was for another person.

Analyses

For each regression analysis, one of the seven groups of measures was entered as the independent variable. One dependent variable was entered per regression. Using a Bonferroni correction the probability for each comparison was corrected to $p < .007$ to accommodate the number of tests conducted. For disclosure, seven regressions were conducted for each of the dependent measures: overall disclosure, disclosure of Personal

identity information, Sensitive personal information, and Stigmatizing information, and disclosure within eight content areas of Facebook (Personal information, Picture and Album information, Work information, Education information, Age information, Contact information, View information, and Relationship information). For privacy settings seven binary logistic regressions were conducted to examine whether the measures predicted the likelihood of employing settings or not (dichotomous scoring). Following, seven linear regressions were conducted to examine whether the measures predicted the number of privacy settings that were changed.

Overall Disclosure. To address the question of which variables predicted disclosure overall, seven linear regressions were conducted. Results revealed that none of the seven regressions were significant.

Disclosure of Personal Identity Information, Sensitive Personal Information, and Stigmatizing Information. To address the question of which variables predicted disclosure in three categories (Personal identity information, Sensitive personal information, and Stigmatizing information), linear regressions were conducted. Results revealed that one linear regression was significant. Specifically, positive attitudes towards computers was a significant predictor of disclosure of personal identity information (t (224) = 3.03, p = .003, R^2 = .04). As positive attitudes towards computers increased, so did disclosure of personal identity information. No other regressions significantly predicted disclosure of either sensitive information or stigmatizing information.

Disclosure within Facebook Content Areas. To address the question of which variables predicted disclosure in eight content areas within Facebook (Personal information, Picture and Album information, Work information, Education information, Age information, Contact information, View information, and Relationship information), linear regressions were conducted.

Results revealed that none of the regressions were significant at the .007 level. While not significant, there was a trend (at the .07 level) such that increased positive attitudes towards computers were related to a greater likelihood of disclosing both education and address information.

Privacy Settings Use. Even given that there was a relatively small percentage of participants who made at least one setting change (approx. 20%), it was important to examine factors related to privacy settings behaviours. It was not surprising that so few participants made any privacy settings changes, as previous research has indicated that this tends to be the case (e.g., Berendt, Gunther, & Spiekermann, 2005; Gross & Acquisti, 2006; Milne & Culnan, 2004). The current analysis sought to examine, within the constraints of the small study sample, which variables predicted privacy settings usage. To do this, seven binary and seven linear regressions were conducted. Binary regressions results revealed that none of the seven groups of measures predicted whether or not privacy settings were employed. When specific number of settings employed was examined, four out of seven linear regressions were significant. Specifically, results showed that private self-consciousness, reported self-disclosure, social desirability: impression management and the virtual other: other referents significantly predicted use

of privacy settings (t (205) = 2.44, p = .02, R^2 = .09, t (220) = 2.30, p = .02, R^2 = .03, t (193) = 1.96, p = .05, R^2 = .03 and t (2, 206) = 2.70, p = .01, R^2 = .04, for private self-consciousness, reported self-disclosure, social desirability: impression management and the virtual other: other referents, respectively). In all cases, as these variables increased, so did use of privacy settings.

Question 3

Effect of Media (Context) and Gender

Design

A third set of analyses was conducted to examine the impact of media condition. Specifically, a 2 (Context condition: Paper-and-pencil, Online) x 2 (Participant gender: Male, Female) x 2 (Target gender: Male, Female) experimental design was employed.

Analyses

Analyses explored whether any differences in disclosure and use of settings in Facebook emerged as a function of context condition, gender of target and gender of participant[9]. Examination of these variables was carried out using univariate and multivariate analyses of variance (MANOVA). Three analyses were conducted for disclosure: one for overall disclosure, one for disclosure divided into three grouping categories (Personal identity information, Sensitive personal information, and

[9] In order to examine disclosure as a function of privacy settings usage, all analyses examining context and gender were repeated using only those participants who did not employ settings. Patterns were consistent with results found for the entire sample.

Stigmatizing information), and one for disclosure within eight content areas with Facebook (Personal information, Picture and Album information, Work information, Education information, Age information, Contact information, View information, and Relationship information). Privacy settings were examined using regression analyses.

Overall Disclosure. A univariate analysis of variance was conducted to examine overall disclosure within the Facebook profiles. Context condition, gender of target and gender of participant were entered as the between subjects factors, and overall disclosure in Facebook was entered as the dependent variable. Results revealed a significant main effect of context, such that participants who filled out their profiles on paper-and-pencil included significantly more information overall than did participants who filled out their profiles online (See Table 26).

Disclosure of Personal Identity Information, Sensitive Personal Information, and Stigmatizing Information. To address the question of how much information participants disclosed in three disclosure categories (personal identity information, sensitive personal information, and stigmatizing information), a multivariate analysis of variance was conducted. Context, gender of target and gender of participant were entered as the fixed factors, and disclosure in each of the three categories were entered as the dependent variables. Results revealed a significant main effect of context for sensitive information only (See Table 27). Participants who filled out paper-and-pencil profiles disclosed more sensitive information than those who filled out profiles online. While results indicated that there were no significant main effects of gender, there was a significant interaction of gender of participant by gender of target for stigmatizing

information in particular. Follow-up independent t-tests revealed that the difference was significant for female targets, (t (129) = 2.34, p = .02), such that male participants disclosed more stigmatizing information about a female target than did female participants (see Table 27).

Disclosure within Facebook Content Areas. To address the question of how much information participants disclosed in eight content areas within Facebook (Personal information, Picture and Album information, Work information, Education information, Age information, Contact information, View information, and Relationship information), a multivariate analysis of variance (MANOVA) was conducted. Context condition, gender of target and gender of participant were entered as the fixed factors, and all eight topics were entered as the dependent variables.

Results revealed that there were significant main effects of context condition for three of the eight topics. Specifically, for relationship information (F (1, 216) = 6.86, p = .009), work information (F (1, 216) = 17.71, p < .001) and contact information (F (1, 216) = 26.95, p < .001). In all three topic areas, disclosure was significantly greater in the paper-and-pencil condition as compared to the online condition (see Table 29). There were no significant main effects for either gender of the participant or gender of the target (largest F = 2.95).

In total, there were four significant interactions. First, there were significant interaction effects of context condition and gender of the participant for education information (F (1, 216) = 7.81, p = .01) and personal information (F (1, 216) = 3.99, p = .05). Follow-up independent t-tests were conducted, one for paper-and-pencil and one for

online, to identify where the differences were occurring. For each, gender was entered as the grouping variable, and education and personal information were entered as the dependent variables. On paper-and-pencil, males disclosed more education information than females (t (127) = 2.36, p = .02, *Mmale* = .63 and *Mfemale*= .49). In comparison, when online, males disclosed more personal information than females (t (101) = 2.19, p = .03, *Mmale* = .60 and *Mfemale*= .48).

Second, there were significant interaction effects of gender of the participant and gender of the target for relationship information (F (1, 216) = 7.35, p = .01) and view information (F (1, 216) = 6.38, p = .01). For relationship information, follow-up independent t-tests were conducted, one for males and one for females, to identify where the differences were occurring. For each, gender of the target was entered as the grouping variable, and relationship information was entered as the dependent variable. Disclosure of relationship information differed by target gender for females only (t (134) = 2.07, p = .04), such that they disclosed more for male targets (*Mmalechar* = .67) than for female targets (*Mfemalechar* = .52).

For view information, follow-up independent t-tests were conducted, one for female targets and one for male targets, to identify where the differences were occurring. For each, gender of the participant was entered as the grouping variable, and view information was entered as the dependent variable. Disclosure of view information differed by gender of participant for female targets only (t (130) = 2.70, p = .008), such that males disclosed more (*Mmale* = .60) than did females (*Mfemale* = .38).

Privacy Settings Use. Preliminary analyses indicated that each condition had at least two participants who employed privacy settings (see Table 30). Due to small cell sizes, this analysis was descriptive in nature. A count was conducted to compare privacy settings by context condition, and revealed that more privacy settings were employed in the paper-and-pencil condition as compared to the online condition. In terms of gender of the participant, females tended to employ more settings than did males. For target gender, females employed far more settings for a target of the same gender. Finally, females in the paper-and-pencil condition employed more settings for female targets in particular (See Table 30).

Discussion

What is Disclosed: Effect of Story and Gender

Overall Disclosure

Overall, in keeping with findings from Study 1 B examination of overall disclosure did not yield significant findings in Study 2, therefore further reinforcing the need to assess disclosure in terms of specific disclosure categories, as well as by topic.

However, important outcomes related to the type of story, gender, and subsequent disclosure were apparent in Study 2. First, while hypotheses 1 and 2 were not supported statistically, the Personal Privacy Story resulted in the lowest amount of overall disclosure, followed by the Legal Privacy Agreement Story and finally the History of the Internet Control Story, which contained the highest amount of disclosure. This pattern is in the hypothesized direction, albeit not significant. It could be that the stories, especially the Personal Privacy Story, were salient but not as salient as they might have been with

more detail and perhaps gender specific information. Perhaps the impact of stories about both genders or stories that depict a variety of scenarios and incidences of privacy invasion resulting from over-disclosure rather than a single instance is worthy of investigation. In addition, if the stories had contained more vivid and negative outcomes as a result of the over-disclosure, the patterns of results may have been strengthened. Alternatively, it may be more important to examine the type of information, as will be conducted below, that can be inhibited as a function of the story rather than sheer quantity, as some types of information may be more risky to disclose than others.

Personal Identity Information, Sensitive Personal Information and Stigmatizing Information

In terms of the three disclosure categories, there were significant differences in disclosure of both sensitive and stigmatizing information in particular. First, female participants disclosed significantly more sensitive information in the History of the Internet Control Story, and significantly less sensitive information in the Legal Privacy Agreement Story. While it was originally hypothesized (see hypothesis 5) that the Personal Privacy Story would have the greatest impact on disclosure for females in particular, it appears that for females there was something especially salient about a legal document. Gender norms are not supportive of female criminality (Steffensmeier & Allan, 1996), and favour instead a motherly, caring and responsible image of females. In addition, females are raised to be moral, nurturing individuals with a strong "ethic of care", or in other words, a strong sensitivity to the needs of others (Gilligan, 1982). It is speculated that, due to moral development and socialization processes, females may be

more inclined to abide by rules and regulations that are framed in a legal way. Therefore, the strength of a legal privacy policy may be augmented for females, thus resulting in less disclosure in this condition in particular.

Alternatively, it is also possible that the legal document was seen as more formal, and as a result, female participants in particular took this story more seriously, resulting in less disclosure. Second, in regards to stigmatizing information, male participants in particular disclosed significantly more for a female target. While not significant, there was also a similar trend for female participants, such that they tended to disclose more for a male target. Even though the information provided did not convey minority status (e.g., homosexual orientation, or extremist political or religious views), examination of less extreme information that could be used to potentially stigmatize another person (even including fairly common religious and political views) was of interest and may still be viewed as threatening. As a result, this information may activate collective group identification (Tajfel, 1982) and even an inclination to protect one's own gender. In this case, both genders may elicit behaviours that reflect a greater value for their own gender, thus limiting disclosure of potentially damaging information. Alternatively, perhaps the participants identify more with the target of the same gender and act in accordance with their own disclosure needs. More specifically, it could be that participants are acting as though the information they are disclosing about the target is in fact information about them, and, therefore, limit sharing information that could be used to humiliate or discredit when the gender of the target matches their own gender.

Different Topic Categories

When disclosure of specific topics was examined, interesting results emerged for two out of the eight topic scales: contact information and view information. Male participants tended to disclose more contact information overall than did female participants. This finding is consistent with research that has found that male disclosure may be topic dependent (Derlega, Durham, Gockel & Sholis, 1981). It is also suggested that males may also be more comfortable disclosing topics that are more prohibited, including contact information. Moreover, it may be that females are more cautious and feel a greater sense of social responsibility (Gilligan, 1982); especially in the case where information is being disclosed for another person they have never met.

While males were more likely than females to disclose contact information for another person, disclosure was also dependent on story. Surprisingly, males who read a control story about the history of the Internet disclosed less contact information than males who read either the Personal Privacy or Legal Agreement stories. This finding was unexpected and surprising as the two other conditions were specifically designed to reduce not increase disclosure. This may be a spurious finding. Alternatively, after reading the History of the Internet Control story, which was really not about Facebook and generally not personally interesting, it could be that this may have made the task less interesting or engaging. This may have resulted in less overall involvement in the task, and may have been especially so for the males in the sample.

There were important interactions between story and target gender. In partial support for hypothesis 5, results demonstrated that the Personal Privacy Story resulted in

less disclosure of contact information for female targets. Moreover, male participants seemed to be particularly sensitive to the gender of the target, and disclosed less contact details for female targets than for male targets, offering partial support for hypothesis 4. While this is not entirely surprising given that the story depicted an incidence in which a female was located and confronted by a reporter based on disclosure of personal contact details, this does reinforce the idea that perhaps females are viewed as more vulnerable and even less competent (Diekman & Eagly, 2000), especially by males, and as such disclosures that could result in bodily harm or potential physical harassment are more carefully considered.

Differences also emerged for political and religious views. Specifically, male participants disclosed more view information about a female target than did female participants. This finding is not surprising given that both political and religious views were included in the stigmatizing information scale and these findings are consistent with results obtained for the disclosure categories, such that males disclosed more stigmatizing information for a female target. In addition, this is also somewhat consistent with findings from Study 1 C where results confirmed that males expressed more information about political and religious views overall than did females, albeit in Study 2 this is intensified for female targets in particular.

Privacy Settings

Not surprisingly, only 20.3% of participants chose to employ at least one privacy setting. This is consistent with previous studies that found that very few users chose to employ privacy settings (e.g., Berendt, Gunther, & Spiekermann, 2005; Gross &

Acquisti, 2006; Milne & Culnan, 2004). In support for hypothesis 5, as expected, by means of a descriptive count, more settings were employed in the privacy invasion story condition that in either of the other two story conditions. Moreover, as anticipated, females tended to employ more settings than males. Interestingly, both genders employed more settings for a target of the same gender. Consistent with the findings from Study 2 examining disclosure, it appears as though males and females alike are more protective of targets of the same gender. Lastly, as predicted, females who read the privacy invasion story employed more settings for female targets. This finding is not surprising given that the story retold an incidence of privacy invasion occurring to a female, thus, perhaps encouraging female participants to engage in more protective behaviours for a female target in particular. The next step might be to provide participants with explicit privacy settings training and instruction, which would encourage use of settings and foster a greater understanding of the options available to users.

Additional Exploratory Factors Related to Disclosure and Privacy Settings Use

A secondary exploratory examination of additional predictors was conducted to assess the predictive power of various factors including: personality, familiarity with technology, attitudes and behaviours related to online privacy protection and the virtual audience. Although previous research has examined factors related to use of technology (e.g., Buchanan, Paine, Joinson & Reips, 2007; Mueller, Wood, Willoughby, Ross & Specht, 2008; Ross, Orr, Sisic, Arseneault, Simmering & Orr, 2009), no known studies have explored novel predictors such as the virtual audience.

Disclosure

While none of the exploratory factors were related to overall disclosure, results indicated that one factor, possessing positive attitudes towards computers in general, was a significant predictor of disclosure of personal identity information. This finding is consistent with previous studies that have looked at how attitudes towards technology relate to use of technology (Levine & Donitsa-Schmidt, 1998; Mueller, Wood, Willoughby, Ross & Specht, 2008). Perhaps possessing positive attitudes about technology encourages greater disclosure by buffering fears of information invasion because users feel more comfortable about their ability to protect themselves, and possibly have a better understanding of technology in the first place. Moreover, it is possible that because those individuals with more positive attitudes are more likely to use technology, the compounding effect of positive experiences with technology and fewer incidences of problems over time may encourage greater disclosure when using the technology.

Interestingly, none of the other factors were related to disclosure. This begs the question; what else drives disclosure? In the current sample, a large majority of participants were university aged students. Following from Erikson's theory of psychosocial development (1968), it is possible that users in this age group possesses a certain degree of naiveté about the self and may not have yet achieved a firm sense of identity (Jensen Arnett, 2000). As a result, these younger users may possess a greater desire for gratification and require more feedback from peers. As such, disclosure of personal details overshadows the requirement for information protection or censorship of

personal details. Even if self-presentation occurs online, and only positive attributes or the ideal self is conveyed, this may be putting users at risk of identity and security breaches. In comparison, older users may have a firmer sense of who they are, and may not possess the desire to disclose to the same degree as their younger counterparts. It is also possible that motivation to use the site differs between groups. For example, perhaps older users are using the site for the purpose of social connectivity, and for keeping in touch with close others within their tight social sphere. In comparison, it could be that younger users are using the site for a means to explore their possible selves and to self-express. While this question was not answered in the current research, it is an area that merits further examination. Lastly, the notion of "culture" is one that may prove important in understanding disclosive communication online. Altman (1975) posited that individuals adjust privacy regulation according to both the environment and the internal state. He went on to acknowledge the importance of the social world, and the context in which privacy is negotiated. For some, Facebook may be considered a "culture", such that certain groups achieve a collective identity whereby standards of disclosure and access to information are set by the group (or the social world), not the individual. Consequently, users within these subcultures on Facebook may be inclined to act in a way that is consistent with what other users are doing. Not only do they act in accordance with the groups norms, this may even instill a sense of normalcy, indicating that if everyone else is doing it, it must be okay. While self-presentation may be viewed as a buffer against presenting more harmful information, given that when self-presenting, information tends to be idealized and more positive (Goffman, 1959), group standards

may dictate what is considered "ideal". If ideal information as set out by the subculture is information that puts the user at particular risk (e.g., posting drunk pictures or pictures of the user in compromising positions), problems may arise. At the same time, perhaps a desire for social acceptance within one's culture overrides rational thought about protecting personal information, and results in over-disclosure of personal information.

There is obvious need for further exploration of additional factors. Even so, while the majority of the factors measured in the current study did not relate to disclosure, they may be associated with privacy settings use. This possibility was explored next.

Privacy Settings

In terms of settings, results revealed that the overall amount of variance in use of privacy settings predicted by the additional exploratory factors was quite small (R^2 = .19). Even so, personality factors including private self-consciousness and social desirability: impression management did significantly relate to increased settings use. Perhaps in the case of private self-consciousness, participants who score higher on this measure may have been more self-reflective, and consequently more concerned with how their information might be used. As a result, they were also more likely to employ settings. Public self-consciousness, on the other hand, was not a significant predictor of settings use. Given that the premise of Facebook is based on creation of personal profiles and displaying personal information, perhaps Facebook itself is not viewed as public by some. It could be that for some users, creating a Facebook account is considered a more private activity. In addition, even despite the fact that Facebook is designed as a site for information sharing, this sharing may be considered to occur only within tight social

networks or within one's personal sphere. Therefore, whether or not one has a public focus does not relate to use of various features of the site. For social desirability, it is possible that participants detected the importance of privacy settings as a feature of the study, and, as such, utilized more of the available privacy settings. Alternatively, Paulhus (1984) views impression management as reflective of a more communal concern in individuals. As such, those who score higher on this scale may be more cautious about their actions, especially when their actions involve others.

Worthy of note, although accounting for a small percentage of variance in privacy settings, the virtual audience and, in particular, having referents in mind other than the self or close friends was significantly related to greater use of privacy settings. Although weak, this finding may be considered encouraging since it seems as though users are more conscious about employing settings when less close others are in mind, but it is still a concern that friends are not considered to be a potential risk. In the case of Facebook, the inability to control accessibility of information displayed by friends may indirectly expose users to the risk of identity theft, and social and personal security issues. For example, if a friend tagged the user in their profile or in an album, and this friend did not have strict privacy settings employed, thus allowing for access to photos, the photos of the user are available to whoever the friend has in their friends list. If friends were considered more of a threat, users may be more likely to employ stricter settings so as to limit what friends can do with their information. For example, users can employ privacy settings that limit what content friends can view. By creating a group that contains only specific users (i.e., friends), users have the option to specify exactly which pieces of

information each group can see, thus selectively limiting access to certain content and indirectly limiting unwanted exposure of information via friends profiles. This previously overlooked area may prove to be especially important in understanding further how users perceive relationships and information sharing online, and how they may be putting themselves at risk unknowingly, but studying this factor may require revised approaches. In the current study, participants were asked about who they were thinking about when simply posting personally revealing information. While they were asked about the referent, participants were not asked about how each referent related to disclosure of specific kinds of information (e.g., photos, status updates etc.). Results may produce significant associations between virtual other and disclosure if topic of disclosure is broken down more finely. In addition, the virtual other may be a concern more so when the information is being posted about the self and not for another person, as in the case of the current study. For both disclosure and use of privacy settings a more in-depth and rich investigation of the dynamics and perceptions of various relationships both while online and offline and how they impact on disclosure and privacy settings use may prove insightful. The next step may be to conduct interviews, and ask users about their choices when posting specific kinds of personal information about themselves, at the time that the information is being posted, and who and/or what they are thinking about when employing specific settings.

Descriptive examination of overall use and effectiveness of the provided privacy settings booklet yielded interesting results. When asked why they did not use the booklet, of those who gave a response, 40.1% participants indicated that they already knew the

settings. Even despite reporting knowing about the settings, and thus having no need to use the booklet, more than a quarter of these participants (25.7%) indicated that they learned something new about the settings that they previously did not know. This highlights the discrepancy between what users are saying they know and what they actually know. Is it possible that this effect reflects age or cohort differences in terms of understanding how much one knows in a certain domain (Dunning, Johnson, Ehrlinger & Kruger, 2003). Presumably, as age increases so does experience and knowledge. Conceivably, those in their late teens or early adult years could have insufficient knowledge or expertise necessary to deduce what they know, and more importantly what they *don't* know. In the case of privacy settings, these individuals may reflect an overconfidence or overestimation of their true knowledge.

Alternatively, it may be that users tend to go with the default, and fail to actively change the settings within Facebook. Users may be more inclined to go with the default option, either because they do not wish to actively change the option, or because it requires a certain level of engagement. Because settings are not presented in such a way that they are readily accessible, perhaps users perceive the task of employing settings as arduous. Without proper knowledge and the desire to explore available privacy options due to inaccessibility and incomprehensible explanations, as in the case of privacy policies, users are left to fend for themselves. In such cases, it appears that this results in a lack of use of settings entirely. This may indicate a need for more effective and comprehensive privacy settings training.

Effect of Media Context and Gender

In order to gain a better understanding of how disclosure of information in traditional formats compares with disclosure online, the impact of media context on disclosure of information was examined. In addition, no known studies have compared privacy settings use across context, and, therefore, this novel area was also examined.

Disclosure

Contrary to expectations (hypothesis 7) and previous studies (e.g., Joinson, 2001; Locke & Gilbert, 1995; Tidwell & Walther, 2002; Wood, Nosko, Desmarais, Ross & Irvine, 2006), overall disclosure was greater on paper-and-pencil than online. This finding was quite surprising. It is possible that because the information was being disclosed for another individual and not for the participants themselves, there may have been a greater concern about the security of the information. This may be supported by the qualitative comments given by participants that reflected a strong sense of responsibility as well as hesitation over their disclosures, because the information was not their own. In the case of online information sharing, perhaps participants felt that this context in particular was more risky than simply writing personal details down on paper. Generally, studies have looked at disclosure specific to the self, such as in the case of survey material about personal opinions, attitudes and behaviours (e.g., Christofides, Muise & Desmarais, 2009). Patterns of disclosure across context, especially when online, may therefore be different when the information is being shared about someone else, especially a complete stranger. On the other hand, perhaps the knowledge or worry of information leakage is greater in an online setting, where not only the researchers have

access to the information, but potentially hundreds if not thousands of other users. This awareness or realization that exposure is greater online may give rise to greater vigilance when disclosing in this context. Alternatively, the nature of the paper-and-pencil booklet may have encouraged greater disclosure. Specifically, participants were given numerous screenshots in a booklet that was visible in its entirety. In contrast to online, where users must scroll through pull down tabs to access similar pages, perhaps the fact that the information was presented directly in front of the participants encouraged them to fill in more. It is also possible that the paper-and-pencil condition was not an authentic task, and was not as comparable to online as previously expected. A potential next step may be to have participants simply fill out profile information on a blank sheet, without the aid of a premade booklet. By allowing them to add in without as many obvious prompts, a better gauge of disclosure in this context may be obtained.

Personal Identity Information, Sensitive Personal Information and Stigmatizing Information

A similar pattern emerged for one out of the three disclosure categories: sensitive information. More sensitive information was disclosed on paper-and-pencil than online. Again, there may be something specific to the information disclosed in the sensitive information disclosure category that is viewed as particularly risky, especially when disclosed online. Further explanation is provided in the next section. In addition, there was also a significant interaction of gender of participant by gender of target for stigmatizing information. Specifically, male participants disclosed significantly more and

female participants significantly less for a female target. These patterns are identical to those found in part 1 examining effect of story and gender.

Different Topic Categories

There were significant main effects of context for three of the eight topics, including work, relationship and contact information. Consistent with findings for disclosure overall and by disclosure category, disclosure of these topics was greater on paper-and-pencil than online. Perhaps sensitive information and these topic areas in particular are considered quite delicate in nature, given that they open up the user to breaches in personal and financial security. For example, sensitive information consisted of various items including information pertaining to one's employer and job position. Not surprising then, disclosure of work information was less online. It is suggested that disclosing contact information and work information may place users at risk of harassment and potentially loss of employment should employers access the information and feel the employee is reflecting inappropriate behavior online. In the case of relationship information, close others including romantic partners and family may also be placed at risk indirectly should they be located or otherwise identified via information found online. There could be something specific to certain content that is considered more unsafe to share, especially when online.

Significant interactions also emerged between context and gender of participant for two of the eight topic scales: education information and personal information. On paper-and-pencil, males disclosed more education information than females. In comparison, when online, males disclosed more personal information than females. This

finding was quite puzzling, given the argument that certain types of information may be seen as more 'unsafe' than others. In the case of education information versus personal information, one might assume that personal information is more risky to share online than education information. It is proposed that, for some, online social networking profiles may be viewed as a less explicit way of meeting romantic partners and may even be seen as a less overt dating site. Even despite the fact that the target person was in a romantic relationship, perhaps for male participants in particular, this was an opportunity to share potentially desirable and insightful information about the target person that could potentially be used in future for dating purposes. Previous research examining gender differences in attitudes towards infidelity has found that males possessed more permissive attitudes (Lieberman, 1988) and also had a stronger desire to engage in unfaithful behavior (Prins, Buunk & VanYperen, 1993). By advertising information such as interests, activities and all "about me", items that were included in the personal information topic scale, it is speculated that perhaps male participants may have been "putting it out there" for the target and displaying information that another user may be interested in knowing should they be looking for a relationship.

Finally, significant interactions emerged between gender of the participant and gender of the target for two of the topic scales: relationship information and view information. Findings revealed that disclosure of relationship information differed by target gender for females only, such that they disclosed more for male targets than for female targets. While this explanation is speculative, this may be a way for females to assert romantic status and faithfulness in the relationship, especially for the male target.

This argument stems from a similar argument made for increased disclosure of personal information online on the part of male participants. Males and females may view relationships differently, such that females may have less permissive attitudes about infidelity and may have an increased need to display this qualifying information, whereas males may view certain interactions as an opportunity to potentially meet new partners. Madden and Lenhart (2006) have found that relationship seekers often use the Internet as a means for locating potential dating partners. In terms of gender, Golub and colleagues (2007) found that males were more likely to report that they would consider dating someone online.

Privacy Settings

When privacy settings were examined descriptively, results revealed that more settings were employed on paper-and-pencil. Again, the nature of the paper-and-pencil booklet may have encouraged greater use of privacy settings. It is possible that users find it overwhelming to find the appropriate setting online, even when a booklet outlining the settings was provided. Moreover, given that online the settings are oftentimes not obviously laid out or in intuitive places, users may have grown tired of looking or decided that it was not worth the effort to locate and employ to appropriate setting.

Offering partial support for hypothesis 2, based on a descriptive count, females employed more privacy settings than did males. This may reflect a general caution on the part of females, and along a similar vein, a greater sense of social responsibility, especially in the case of a stranger's personal information. For gender of the target person, females employed more settings for a target person of the same gender. This

result is consistent with results regarding disclosure in Study 2, albeit this finding only applies to females. Finally, females in the paper-and-pencil condition employed more settings for female targets in particular. Given the relatively larger amount of disclosure on paper-and-pencil, it appears as though females are more consistent in their protective behaviours. While results were descriptive in nature, it is possible that females in particular are more inclined to complement their disclosure with use of privacy settings. This possibility warrants further examination.

Summary

Although the effect of story was not as strong as hoped, overall, this study provides partial evidence that having participants read certain stories may encourage them to alter the way in which they display or share personal information, even in the case of information about another person. Given the relative lack of impact of privacy policies on over-disclosure, results from this study may help give insight into more effective ways of reaching a potentially at risk population. In addition, this study offers insight into differences in information sharing across context, and provides evidence that previously found patterns of self-disclosure may not be consistent when the information is being disclosed for another person.

Study 1 B and C did not yield significant gender differences in disclosure, while in Study 2 gender played a significant role. Not only did males and females differ in disclosure, but consideration of the gender of the target seems to be important in understanding what types of information in particular people are willing to share about another person.

In contrast to Study 1 C, in Study 2 contact information and personal information emerged as key topics of disclosure, suggesting that there is utility in examining factors including story, context and gender in reference to specific content.

Lastly, while a small percentage of the sample chose to employ privacy settings, this was not a surprise. However, for those who did choose to employ privacy settings, there were descriptive associations with the type of story read. While effect of story was not as strong as hoped, the results from Study 2 highlight how a salient anecdotal story could predict increased use of privacy enhancing features. There was also a gender trend consistent with previous research (Kehoe et al., 1997; O'Neil, 2001; Youn & Hall, 2008) whereby females demonstrated greater use of privacy settings, especially when displaying information for another female. In sum, in comparison to disclosure, similar factors were related to use of privacy settings. Given the relative lack of research examining story, gender and privacy settings use, the current study offers a first glance at factors that may be associated with an increase in privacy settings use in personal profiles.

General Discussion

Studies 1 A, B, and C provided an initial, systematic exploration of Facebook profiles. The study identified what kinds of information can be disclosed through these profiles, as well as when information is likely to be disclosed, and by whom.

Specifically, the first contribution of these studies was the construction of a comprehensive checklist to identify the types of information available on the Facebook profiles. This first step was important for establishing a general checklist that can be

used in future Facebook research. No known checklist that accounted for all of the possible items contained within online Facebook profiles existed prior to this research. Developing this tool was a first step in permitting systematic study of what is and is not disclosed on social networking profiles. Analysis of the information assessed by this checklist indicated that there is a great diversity of kinds of information that can be shared and that, for some online social networking users, a great deal of information is shared through this media and that some information is more likely to be revealed than others. Information provided in Study 1 A established that there was information that could be considered both threatening and non-threatening to users. Once this was established, the purpose of Study 1 B was then to further examine factors that predicted disclosure within the more threatening information categories. Developing this instrument and then refining the instrument through the categories identified in Studies 1 A, B, and C represents a substantial contribution to existing research as the categories provide a systematic mechanism though which subsequent research can assess the quantity, types and potential risk that disclosed information represents.

Study 2 was an initial systematic investigation using the tools developed from Studies 1 A, B, and C and examined experimentally the impact of story, gender and media context on overall disclosure and use of privacy settings. Understanding mechanisms by which individuals will disclose more 'safely' online is a key concern today. Study 2 broadened awareness of potential factors that may help to inhibit over-disclosure and the subsequent risk of information invasion in personal profiles, and indicated a need for further examination of additional factors that may be related to use

of settings. Gender in particular emerged as a very strong predictor of disclosure across a variety of topic areas. While Study 2 produced some surprising findings, this may indicate a need for further examination of the association between various factors.

Keeping in mind that disclosure was for a target person, it appears that patterns of disclosure in social networking sites such as Facebook may be different from disclosure patterns found in more traditional studies. Typically, disclosure occurs in the case where two or more individual already know each other, and where a conversational "back and forth" occurs, such as in the case of reciprocal information sharing. Online, and more specifically in the case of Facebook, this back and forth is not as evident. In fact, in most cases disclosure occurs whereby information is broadcasted to other users, but there is not always feedback or follow-up from an interaction partner.

In the current study, gender emerged as a strong predictor of disclosure for another person. Traditional self-disclosure theory boasts strong gender differences in terms of communication patterns, with females disclosing more than males (Dindia & Allen, 1992). Results from the current study did not support this and instead revealed that females consistently censored their disclosures for a target individual more than did males across a variety of different topics. In the case of disclosure for another person, gendered communication appears to be different in social networking profiles as compared to face-to-face. These findings may inform current theory, and may call for revision to traditional explanations of disclosure by gender.

Careful revision may be required to tailor existing theories of disclosure offline to fit disclosure online. For example, while speculative, the order of the stages in the theory

of social penetration (Altman & Taylor, 1973) may require revision. In terms of personal disclosure in social networking sites such as Facebook, it may be that the orientation stage whereby people are more cautious about the types of information they divulge, occurs later on and may be prompted by incidences involving invasion of privacy or greater experience with the site. At first rather, it appears that there is a moderate level of disclosure containing both more risky and less risky information, consistent with both the exploratory affective stage where people begin to express basic opinions (e.g., their political opinions), and the affective stage where even more intimate details are revealed. Given that this theory typically addresses the "getting to know" process in a relationship, in the case of personal disclosure on Facebook where presumably most users already know their audience, similar stages of communication may occur, but in a slightly different order.

Current theories of online communication such as the hyper-personal theory of online communication have attempted to explain online relationships that are formed and maintained solely online. This theory in particular may require revision to include relationships that are formed offline and maintained solely online, as in the case of relationships on Facebook. The "getting to know" process may not apply in these relationships. Furthermore, examination and consideration of how personal self-disclosure online (i.e., when users post information without the expectation of direct reciprocal communication) occurs and differs from relational self-disclosure is necessary. Features that are important in explaining disclosure relationally may not apply or may require revision when applied to personal disclosure online in social networking profiles.

While pitfalls exist in existing online theory, there are a variety of components that can be applied to personal disclosure in social networking profiles, including asynchronous time, reduced cues and the norm of reciprocity. First, Facebook users have opportunities to communicate through various means, including an email inbox or by posting on another users' wall. In both cases, response from other users is not immediate and therefore, consistent with the notion of asynchronous time, a lag time in between messages exists. In this case, users may filter and censor their disclosure messages. Second, communication via Facebook profiles often occurs in text-based form, but is not limited to text. Users have the opportunity to convey meaning through use of emoticons, graphics, and pictures. Therefore, while there are reduced cues when communicating online (e.g., lack of physical cues including gestures, tone and intonation), the cues presented by communication partners are not as "reduced" or strict as originally set forth by Walther (1996). This may be worthwhile considering. Third, the norm of reciprocity, which refers to the expectation that disclosure will be returned at a comparable level applies to personal disclosure via social networking profiles. This may be related to the idea of a "Facebook" culture, whereby users within a specific online social sphere may set out standards for what is expected in terms of personal disclosure. If other users in an individual's friends group post highly personal pictures, intimate status updates and regular wall posts, then that individual may be expected to disclose to the same degree. It may be that the "culture" dictates what is expected as opposed to the interaction partner, as in the case of traditional theories of reciprocal communication (Gouldner, 1960).

While speculative, a variety of other factors that were not examined in the current research may prove useful in understanding the nature of disclosure and privacy settings use in social networking profiles, and may inform current theory. Perceived trust in the system (i.e., how trustworthy the site is perceived to be) may influence decisions about displaying personal information. The consensus is that Facebook is perceived as more trustworthy than other social networking sites, such as MySpace (Fogel & Nehmad, 2009). Given that the site is endorsed as being reliable and safe, users may feel more comfortable disclosing riskier pieces of information. Perceptions of trust in the system therefore warrant further examination in relation to disclosure and privacy settings use. Cues from the social environment on Facebook may also be related to information disclosure. If users are obtaining positive feedback from other users based on the information displayed, the costs and risks of disclosing highly personal details may be overshadowed by the benefits associated with over-disclosure, such as popularity or attention. Moreover, motivation to use the site may play a significant role in disclosure and privacy settings use when online. Individual goals for using the site may vary from one user to the next, including social connectivity, identity exploration, self-esteem, popularity, curiosity, and even revenge. These goals may also drive perceptions of the benefits and costs associated with disclosing information. For example, social exchange theory posits that if benefits outweigh the costs of a particular relationship, disclosure within that relationship increases. Depending on individual motivations, the perceived cost/benefits may vary, and as a result subsequent patterns of disclosure may differ. Furthermore, who the user is thinking about (the virtual other) and the perceived risks

associated with that particular person seeing their information may be related to the amount and type of information displayed as well as the privacy settings employed. Disclosure may be higher for virtual others that are perceived as less threatening (e..g, friends). It could be that users are thinking about various virtual others at the same time. Management of opposing virtual others (e.g., mother and ex-boyfriend) and how users make decisions about what to post ultimately is therefore worthy of exploration, and may also be related to motivation or individual reasons for using the site. Lastly, existence of a common Facebook subculture and the notion of "birds of a feather flock together" may prove particularly useful in understanding disclosure and settings use in social networking profiles. Investigation of the norms and standards that are set out by a particular online culture and how these expectations are transferred to disclosure and settings usage within personal profiles is necessary. While even less if known about privacy settings behavior, the possibility remains that the same factors that explain disclosure may also explain use of protective mechanisms. Ultimately, further research examining factors that relate to self-disclosure and information control processes (i.e., privacy settings use) in more detail is required before revisions to existing theory and creation of new theory can be achieved, but may eventually guide the development of theories of personal disclosure in social networking profiles.

Limitations

Studies 1 A, B, and C examined only those profiles that were publicly accessible, meaning that profiles with privacy settings limiting access were not included in the analysis. It is possible that those users who choose to employ settings are very different

from those who do not (i.e., have publicly accessible profiles). Users with publicly accessible profiles may be more likely to disclose more overall, while those who do not allow for public accessibility may be more inclined to censor certain pieces of information over others. This possibility warrants examination. While this is a limitation, the findings from these studies offer insight into the kinds of information that are being shared, and the factors that help to predict who is more or less likely to over-disclose.

Study 1 A allowed for the development of a comprehensive scoring tool that will guide future research in this area. While this coding scheme was not cross-validated due to time constraints, additional studies employing this coding scheme may prove useful in establishing validity.

Study 2 examined disclosure and privacy settings use when the information was for another person, not the user themselves. While results were not strong, findings suggest that factors previously examined as predictors of technology use may not relate to use of privacy settings. This indicates further examination is needed to identify which factors may have a stronger effect of privacy settings usage. It is suggested that knowledge about the risks and life experiences may have played a role in predicting use of privacy settings. For example, if an individual has gone through life experiences related to identity theft, or has encountered other individuals who have had their identity compromised, they may be more apprehensive about information security when online. In addition, by sampling from a more diverse age group, age may have been related to increased privacy settings usage, with older users exhibiting increased use of privacy

settings. Unfortunately, in the current sample, age was limited and therefore this factor could not be examined as a predictor. It is also possible that motivation and education plays a role in the likelihood to use privacy settings. More specifically, greater exposure to media though news and media stories online and offline and taking an active role in pursuing information about the risks may better predict who is more likely to use the available security features. While information is available about the settings, it is ultimately up to the user to pursue the information, whether it be clicking on a link or actively searching for the privacy policy information. The more educated an individual is about the risks, the more likely they may be to protect themselves. This may also be dependent on the motivation of the user to pursue the information, and could possibly be related again to age and life experiences.

Given that social networking sites are based on information sharing and more importantly, sharing information about others within one's social sphere, understanding what impacts of the likelihood of over-disclosing about someone else is critical. In Study 2, the impact of the anecdotal story was not as strong as hoped. This may be due to the fact that the story did not contain any real negative outcomes as a result of over-disclosure. In the case where some negative consequence was reflected, the saliency of the story may have increased and may have therefore yielded greater differences between stories.

Until replication can be conducted, it is also possible that the effects found in Study 2 were being driven by specific elements of the information provided in the target person's portfolio. For example, it was clear that the target was in the midst of moving to

a different city. In this case, the gender differences found in regards to posting relationship information, such that males posted less and females posted more, could be a by-product of a change in location. By this, it could be that males and females view the commitment aspect of a romantic relationship as dependent on proximity. Perhaps for males, relationships are viewed as less stable when partners are further away from one another (i.e., in different cities). While this is quite speculative, this may be a point to consider for future studies.

Directions for Future Research

Based on findings from the current studies, the next step may be to examine how explicit privacy training impacts on disclosure and privacy settings use. It is apparent that there is a need for additional, more effective ways of educating users about the options available to them when online. This may illustrate why certain users are not employing settings and help inform policy and web developers about better ways of conveying features available to users.

Further, inclusion of different participant groups such as older and younger users and novice and expert users will allow for a more comprehensive look at how various groups use social networking sites. In addition to these possibilities, a follow-up study employing a variety of stories that contain content about both genders, identifying information (e.g., actual names of the victims) and numerous scenarios including both negative and positive outcomes may prove useful in narrowing in on the specific features of anecdotal stories that encourage users to disclose less and better protect themselves and others through use of privacy settings.

Moreover, qualitative examination of content including status updates and text entries (e.g., wall posts) may prove useful in understanding the links between self-disclosure theory and disclosure in an online social networking setting, and may aid in the development of new disclosure theories that apply directly to information sharing in personal profiles. Qualitatively examining text based entries may offer a richer assessment of content of messages conveyed in social networking profiles. By taking into account the differences between disclosure that involves reciprocal communication and direct feedback, and disclosure of information that is simply broadcasted by a user for an audience without expectation of interaction, a clearer understanding of how people are communicating online may be obtained.

In order to gain a more complete picture of disclosure and settings use online, examination of private profiles (i.e., profiles that are not publicly accessible) needs to be conducted. Perhaps disclosure and use of privacy settings is very different in this case. In addition, various other distinguishing factors including familiarity with technology and how long they have been a Facebook member may be associated with use, and therefore merits investigation.

Finally, the virtual other warrants further investigation. It may be of particular utility to conduct interviews with users in order to gain a richer understanding of who and what they are thinking about when posting information and when choosing, or not choosing, to use the available privacy features. By specifically asking users who they are thinking about when posting certain information, at the time that it is posted, will help

researchers to better understand the relationship between the mental audience and activities online in personal profiles.

Table 1.

Frequencies for All Dichotomously Scored Items in the Facebook Checklist

Item	Sub categories within Dichotomous variables	Frequency	N
Can you poke them?		99.30%	397
Can you message them?		99%	396
Mini-Feed		97.50%	390
Profile Picture		91.80%	367
	(Profile Picture) self	73.80%	295
	(Profile Picture) friends	22%	88
	(Profile Picture) relationship partner	11.30%	45
	(Profile Picture) activity	7.30%	29
	(Profile Picture) random picture	7%	28
	(Profile Picture) family	4.50%	18
	(Profile Picture) animal(s)	3.80%	15
	(Profile Picture) school	0.50%	2
	(Profile Picture) work	0.30%	1
Birthday		88%	352
	Birth day	83.80%	335
	Birth year	73.30%	293
Friends Viewable		87.80%	351
College/University		83.30%	333
Wall		83%	332
Gender		82%	328
	(Gender) male	38.80%	155
	(Gender) female	29%	116
Applications		81.50%	326
Groups (joined at least one group)		79.30%	317
Photos of…		77.50%	310
Tagged Photos		75.80%	303
Can you send them a gift?		71.30%	285
Photo Album(s)		70%	280
Relationship Status		63%	252
	(Relationship status) in a relationship	30.30%	121
	(Relationship status) single	23.80%	95
	(Relationship status) married	4.80%	19
	(Relationship status)	3%	12

	engaged		
	(Relationship status)it's complicated	1.30%	5
	(Relationship status) in an open relationship	0%	0
High school		62.80%	251
Concentration		62.30%	249
Graduation Year		56%	224
Self Selected Photos		55.30%	221
Interested in (Sexual Orientation)		54.50%	218
	(Interested in) women	33%	132
	(Interested in) men	22.50%	90
Favorite Music		51.30%	205
Favorite Movies		50.30%	201
Gifts		47.80%	191
Favorite Quotes		47.30%	189
Interests		46.80%	187
Favorite TV Shows		46.80%	187
Hometown		45.40%	182
Email address		43.30%	173
Favorite Books		40.80%	163
Activities		37%	148
Employer		35.3%%	141
Political views		35%	140
Job Listed (have listed at least one job)		32.50%	130
Religious views		32%	128
About Me		30.80%	123
Position		30.50%	122
Status		25.80%	103
Posted Items		25.30%	101
Time Period		24.30%	97
Notes		23.50%	94
Personal Pages		23.50%	94
Looking for (Relationship Preference)		19.50%	78
	(Looking for) friendship	19.80%	78
	(Looking for)relationship	5%	20
	(Looking for)networking	4.80%	19
	(Looking for) dating	4%	16
	(Looking for)whatever I can get	2.50%	10
	(Looking for) random play	2.30%	9

Job Description		17.80%	71
Tagged Videos		13%	52
Fun Wall		9.80%	39
Residence		9.30%	37
Degree		9%	36
	(Degree) Masters	4.50%	18
	(Degree) Bachelors	3.30%	13
	(Degree) Doctorate	2.30%	9
	(Degree) Diploma	1.30%	5
	(Degree) Post-doctorate	0%	0
	(Degree) Alumni	0%	0
Website		8%	32
City/Town		7.80%	31
Former Name		5%	20
Mobile Phone		5%	20
Events (as indicated in their mini-feed)		4.80%	19
Home Address		3.50%	14
Room		3.30%	13
Advanced Wall		3%	12
Super Wall		3%	12
Market Place listings		3%	12
Land Phone		2.30%	9
Courses		2.30%	9
School Mailbox		1.30%	5
Zip		0.80%	3
Awards		0%	0

Table 3.

Means, Standard Deviations and T-test Statistics for Default/standard Information, Sensitive Personal Information and Potentially Stigmatizing Information

Grouping Strategy/ Factor	Mean (SD)	T- test
Default/Standard Information		
Network type		
University	3.12 (1.23)	t (1, 398) = -2 81, p = 005
Community	2.77 (1 23)	
Gender Revealed		
Indicated	3 14 (1 11)	t (1, 398) = -9.92, p < .001*
Not Indicated	1 41 (1.13)	
Gender		
Male	3 23 (1.08)	t (1, 352) = 1 74, p = .08
Female	3 03 (1 14)	
Relationship Status Revealed		
Indicated	3 17 (1.10)	t (1, 398) = -4.94, p < 001*
Not Indicated	2 55 (1.36)	
Age Revealed		
Indicated	1 12 (.88)	t (1, 398) = -3.81, p < 001*
Not Indicated	1.47 (.79)	
Sensitive Personal Information		
Network type		
University	9.63 (2.27)	t (1, 398) = .24, p = .81
Community	9.68 (2.28)	
Gender Revealed		
Indicated	9.92 (2.09)	t (1, 398) = -7 01, p < 001*
Not Indicated	7 57 (2.59)	

Gender		
Male	9 74 (2.18)	t (1, 352) = -1.85, p = 07
Female	10.15 (1.93)	
Relationship Status Revealed		
Indicated	10.05 (1.95)	t (1, 398) = -4.70, p < .001*
Not Indicated	8.97 (2.61)	
Age Revealed		
Indicated	9.86 (2 15)	t (1, 398) = -3 05, p = .002*
Not Indicated	9.09 (2.49)	
Potentially Stigmatizing Information		
Network type		
University	6.80 (3.89)	t (1, 398) = 1 43, p = .15
Community	7.35 (3.71)	
Gender Revealed		
Indicated	7.50 (3.65)	t (1, 398) = -6.63, p < .001*
Not Indicated	3.74 (3.42)	
Gender		
Male	7.84 (3.67)	t (1, 352) = 1.84, p =.06
Female	7.28 (3.58)	
Relationship Status Revealed		
Indicated	7.74 (3.51)	t (1, 398) = -4.73, p < 001*
Not Indicated	5 93 (4.04)	
Age Revealed		
Indicated	7.57 (3.68)	t (1, 398) = -4 36, p < 001*
Not Indicated	5.74 (3.84)	

*Significant at the .003 level

Table 4.

Factor Loadings Based on a Principal Components Analysis with Varimax Rotation for 39 Items

Variable	1	2	3	4	5	6	7	8	9	10	11
Sexual Orientation	0.17	0.15	0.11	0.11	0.00	0.10	0.11	0.05	0.11	-0.07	**0.73**
Looking for	0.16	0.02	0.16	-0.14	-0.04	-0.02	0.08	-0.03	0.10	0.23	**0.70**
Birth Day	-0.03	0.10	0.02	0.10	0.03	0.05	**0.89**	0.04	0.07	0.01	0.13
Birth Year	0.03	0.06	0.01	0.12	0.01	-0.03	**0.89**	-0.05	0.05	-0.05	0.03
Political views	0.16	-0.01	0.14	0.01	0.02	0.06	0.15	0.05	**0.69**	-0.09	0.23
Religious views	0.27	0.05	0.13	-0.02	0.02	0.05	0.02	0.16	**0.66**	0.01	0.01
Address	-0.01	0.00	0.06	0.06	0.06	0.00	-0.03	**0.80**	0.03	0.02	-0.02
City/Town	0.00	0.11	-0.01	0.12	-0.32	0.00	0.06	**0.53**	0.26	-0.03	-0.22
Zip or postal code	0.05	0.01	-0.09	0.02	0.03	0.03	0.00	**0.83**	0.03	-0.02	0.13
Activities	**0.69**	0.06	0.06	0.07	0.02	0.07	-0.02	0.04	0.05	0.04	0.11
Interests	**0.81**	0.08	0.06	0.06	-0.03	0.02	0.08	-0.01	0.08	0.06	0.04
Favorite Music	**0.84**	0.11	0.06	0.05	0.05	0.01	0.01	-0.02	0.04	0.02	0.11

Favorite TV Shows	**0.83**	0.08	0.09	0.00	-0.03	0.02	0.04	-0.04	-0.09	0.02	0.17
Favorite Movies	**0.86**	0.12	0.06	0.04	-0.02	-0.01	0.06	-0.02	-0.03	0.00	0.04
Favorite Books	**0.79**	0.02	0.06	0.06	0.03	0.05	0.03	0.03	0.07	-0.01	-0.03
Favorite Quotes	**0.66**	-0.02	0.06	0.00	-0.03	0.11	-0.06	0.00	0.16	-0.09	-0.05
About Me	**0.66**	0.00	0.08	0.04	-0.08	0.09	-0.12	0.06	0.15	0.02	0.02
College/University	0.00	0.01	0.10	**0.76**	0.04	-0.17	0.11	0.09	-0.18	-0.10	0.00
Concentration	0.10	-0.02	0.08	**0.78**	-0.03	0.04	0.06	0.05	-0.06	-0.13	0.16
Graduation Year	0.09	0.06	0.16	**0.71**	0.06	0.10	0.00	-0.02	0.15	-0.03	-0.16
High School	0.09	-0.01	0.12	**0.69**	-0.02	0.21	0.08	0.05	0.09	0.04	-0.02
Employer	0.08	0.05	**0.89**	0.12	-0.02	-0.04	0.06	-0.01	0.03	0.04	0.05
Job Position	0.08	0.03	**0.90**	0.15	0.00	-0.03	0.04	-0.01	0.04	0.05	0.08
Job Description	0.17	0.05	**0.77**	0.02	0.03	0.02	0.01	-0.01	0.07	0.05	0.02
Job City/Town	0.03	-0.01	**0.49**	0.09	-0.13	0.05	-0.16	0.00	-0.01	-0.15	0.27
Job Time Period	0.11	-0.05	**0.83**	0.11	-0.06	0.08	0.04	0.00	0.10	0.11	-0.01
Photos of…	0.09	**0.85**	0.05	0.02	-0.04	0.22	0.07	0.05	-0.08	-0.04	-0.02

Tagged Photos	0.07	**0.85**	0.07	0.07	0.02	0.26	0.07	0.05	-0.07	-0.05	-0.02
Self-Selected Photos	0.15	**0.54**	0.19	-0.04	0.02	0.41	0.14	0.11	-0.35	-0.12	0.04
Friends Viewable	0.08	**0.70**	-0.02	-0.02	0.16	0.06	0.00	-0.05	0.07	0.11	0.11
Wall	0.05	**0.80**	0.00	-0.10	0.05	-0.13	0.01	0.04	0.05	0.10	-0.01
Groups	0.10	**0.55**	-0.11	0.21	0.13	0.18	0.02	-0.06	0.19	0.15	0.16
Photo Albums	0.09	0.17	0.17	-0.05	0.05	**0.70**	0.23	0.07	-0.26	-0.05	-0.01
Send message	-0.06	0.15	-0.06	0.02	**0.93**	0.06	0.06	0.01	0.03	0.01	-0.06
Poke	-0.02	0.12	-0.05	0.04	**0.94**	0.07	-0.02	-0.01	0.01	0.00	0.01
Profile Picture	0.12	0.26	-0.06	0.23	0.10	**0.65**	-0.12	-0.04	0.19	0.02	0.02
Applications	0.13	0.17	-0.05	0.08	0.03	**0.66**	-0.09	0.00	0.20	0.17	0.09
Fun Wall	0.05	0.05	0.08	-0.06	-0.01	0.02	-0.02	0.02	-0.05	**0.78**	0.00
Super Wall	-0.02	0.08	0.04	-0.09	0.02	0.07	-0.01	-0.02	0.00	**0.77**	0.08

Note Factor loadings > .49 are in boldface

Table 5.

Variables, Mean Scores, and Standard Deviations for Factor Analyzed Content Scales (N = 400)

Scale	Variables Included in Scale	Mean (SD)
Personal information	Activities, Interests, Favorite Music, Favorite TV Shows, Favorite Movies, Favorite Books, Favorite Quotes, and Information "About me"	3.51 (3.07)
Tagged and Self-selected Photos and Update information	Photos of..., Friends viewable, Tagged Photos, Self-Selected Photos, Groups, and Wall	4.50 (1.85)
Work information	Employer, Position, Description, and Time Period	1.80 (1.54)
Education information	College/University, Concentration, Graduation Year, and High School	2.64 (1.41)
Message and Poke information	Send a Private Message, and Poke (nudge)	1.98 (.18)
Album and Profile Picture information	Profile Picture, Photo Albums, and Applications	2.43 (.84)
Age information	Birth Day and Birth Year	1.57 (.76)
Contact information	Address, City/Town, and Zip/Postal Code	.12 (.41)
View information	Political Views, and Religious Views	.67 (.78)
Other Wall Presence	Fun Wall and Super Wall	.13 (.39)
Relationship information	Looking for (relationship, friendship, networking, random play etc), and Sexual Orientation	.74 (.73)

Table 6.

Means, Standard Deviations, and T-test Statistics for Facebook Content Scales as a Function of Network Type, Gender Revealed (indicated/not indicated), Gender (male/female), Relationship Status Revealed (indicated/not indicated), and Age Revealed (indicated/not indicated)

Factor	Mean (SD)	T- test
Network type		
View Information		
University	.56 (.75)	t (1, 398) = 2.84 p = .005*
Community	.78 (.80)	
Gender Revealed		
Personal Information		
Indicated	3.71(3.05)	t (1, 398) = -3.75 p < 001*
Not Indicated	1.93 (2.83)	
Photo and Update		
Information		
Indicated	4.78 (1.60)	t (1, 398) = -6.19 p < 001*
Not Indicated	3.07 (2.33)	
Education Information		
Indicated	2.80 (1.33)	t (1, 398) = -6.61 p < .001*
Not Indicated	1.41 (1.44)	
Photo Album and Profile		
Picture Information		

Indicated	2.53 (.72)	t (1, 398) = -6.46 p < 001*
Not Indicated	1.72 (1.26)	
Age Information		
Indicated	1.64 (.70)	t (1, 398) = -5.61 p < .001*
Not Indicated	1.00 (.94)	
Gender		
View Information		
Male	.93 (.80)	t (1, 352) = 5.58 p < 001*
Female	.48 (.70)	
Relationship Status Revealed		
Personal Information		
Indicated	3.83 (3.01)	t (1, 398) = -2.79 p = .005*
Not Indicated	2.95 (3.10)	
Photo and Update		
Information		
Indicated	4.87 (1.63)	t (1, 398) = -4.08 p < 001*
Not Indicated	4.10 (2.10)	
Photo Album and Profile		
Picture Information		
Indicated	2.57 (.67)	t (1, 398) = -3.86 p < .001*
Not Indicated	2.20 (1.03)	
Age Information		
Indicated	1.68 (.66)	

Not Indicated	1.37 (.87)	t (1, 398) = -3.77 p < 001*
View Information		
Indicated	.77 (.80)	t (1, 398) = -3.37 p =.001*
Not Indicated	.50 (.73)	
Age Revealed		
Education Information Indicated		
	2.78 (1.34)	t (1, 398) = 3.22 p =.001*
Not Indicated		
	2.28 (1.54)	

*Significant at the .005 level

Table 7.

Means and Standard Deviations of Each of the Three Relationship Statuses for Tagged and Self-selected Photos and Update information, Album and Profile Picture information, Age Information, & Work Information

Scale	Single	In a Relationship	Status Missing
Tagged and Self-selected Photos and Update information	4.98 (1.35)	4.81 (1.78)	4.12 (2.08)
Album and Profile Picture information	2.47 (.68)	2.65 (.62)	2.19 (1.03)
Age Information	1.76 (.56)	1.66 (.68)	1 35 (.87)
Work Information	1.38 (1.63)	1.21 (1.57)	.76 (1 40)

Table 8.

Breakdown of Story Condition by Gender of the Target for Male Participants.

		Gender of the Target		
		Male	Female	Total
Story Condition	Legal Privacy	18	15	33
	Personal Privacy	20	15	35
	Internet Control	15	17	32
Total		53	47	100

Table 9.

Breakdown of Story Condition by Gender of the Target for Female Participants.

		Gender of the Target		
		Male	Female	Total
Story Condition	Legal Privacy	15	29	44
	Personal Privacy	17	29	46
	Internet Control	17	29	46
Total		49	87	136

Table 10.

Breakdown of Context Condition by Gender of the Target for Male Participants

		Gender of the Target		
		Male	Female	Total
Context	Paper and pencil	36	19	55
Condition	Online	17	28	45
Total		53	47	100

Table 11.

Breakdown of Context Condition by Gender of the Target for Female Participants

		Gender of the Target		
		Male	Female	Total
Context	Paper and pencil	16	58	74
Condition	Online	33	29	62
Total		49	77	136

Table 12.

Descriptives for all Unstandardized/Newly Created Measures

Scale	N	Range	Min	Max.	Mean	SD
Positive Attitudes Towards Computers	230	16	5	21	17.58	3.63
Concern· Virus	227	48	8	56	38.116	11.85
Concern: Entity	228	30	5	35	24.55	8.09
Software Use Strategy	229	18	3	21	16.22	4.77
Privacy Strategy	227	18	3	21	14.53	3.98
Password Strategy	227	18	3	21	11.96	3.90
Inability to Protect	228	27	5	32	11.99	5.53
No Need for Privacy	230	16	3	19	7.23	3.49
Degree of Disclosure	228	25	3	28	15.29	5.75
Consideration Degree of Disclosure	229	12	3	15	10.08	2 43
Privacy Settings Behaviour	229	18	3	21	13.26	4.68
VIRTUAL OTHER: Myself/Friends	230	12	2	14	9 96	2.80
VIRTUAL OTHER: Other Referents	209	54	9	63	27.77	10.58

Table 13.

Descriptives for Computer Use Scale and Short Privacy Scale.

Scale	Item	N	Range	Min.	Max.	Mean	SD	Frequency (Yes)
Computer Use: How many hours per week do you spend using the computer for:	Internet	230	104	1	105	17.71	15.21	n/a
	Recreation	230	65	0	65	13.35	12.77	n/a
	Work	230	69	1	70	15.93	12.42	n/a
Privacy Survey	Did you notice the booklet? (Y/N)	226	1	0	1	.70	n/a	69.9
	Did you use the booklet? (Y/N)	232	1	0	1	.28	n/a	28
	Did you learn anything new about the settings? (Y/N)	226	1	0	1	.32	n/a	31.9
	How enjoyable did you find the Facebook creation task?	213	6	1	7	5.21	1.12	n/a

Table 14.

Descriptives for all Standardized Measures.

Scale	N	Range	Min.	Max.	Mean	SD
Self Disclosure	229	75	16	91	62.72	14.10
Public Self-Consciousness	227	66	18	84	47.96	11.99
Private Self-Consciousness	228	54	16	70	48.96	10.18
Extraversion	228	6	1	7	5.11	1.31
Agreeableness	227	5	1	7	4.91	1.08
Conscientiousness	226	5	1	7	5.22	1.19
Emotional Stability	227	6	2	7	5.87	1.19
Openness	228	5	2	7	5.57	1.05
BIDR: Impression Management	212	7	1	8	2.35	1.78
BIDR: Self Deceptive Enhancement	208	7	1	8	2.35	1.95
Online Privacy Attitudes	216	94	18	112	68.12	21.48
Online Privacy Behaviours: General Caution	225	32	6	38	18.91	7.57
Online Privacy Behaviours: Technical Protection	221	33	9	42	28.06	7.26
Online Privacy Behaviours: Total	219	63	16	79	46.76	12.42

Table 15.

Number of Privacy Settings as a Function of Story Condition, Gender of the Participant and Gender of the Target

Gender of the Participant	Gender of the Target	Story Condition			
		Legal privacy story	Personal privacy story	History of the internet	Total
Male	Male	1	6	3	10
	Female	2	2	4	8
Female	Male	3	1	2	6
	Female	8	11	6	25
	Total	14	20	15	49

Table 16.

Means, Standard Deviations and F-test Statistics for Overall Disclosure as a Function of Story and Gender

Model	Factor	Mean (SD)	F Test
Overall Disclosure			
	Story		$F(2, 210) = .68, p = .51$
	Personal Privacy	16.60 (6.24)	
	Legal Privacy Agreement	17.08 (6.14)	
	History of the Internet Control	17.89 (5 56)	
	Gender of Target		
	Male	17.47 (6.07)	$F(1, 210) = .12, p = .73$
	Female	16.96 (5.96)	
	Gender of Participant		
	Male	17.85 (6.23)	$F(1, 210) = 1.38, p = 24$
	Female	16.67 (5 79)	
	Story * Gender of Target		$F(2, 210) = .89, p = 41$
	Personal Privacy * Male	17.33 (6.53)	

Personal Privacy * Female	15.98 (6 00)	
Legal Privacy Agreement * Male	17.93 (6.05)	
Legal Privacy Agreement * Female	16.50 (6.20)	
History of the Internet Control * Male	17.17 (5.56)	
History of the Internet Control * Female	18.34 (5.56)	
Story * Gender of Participant		$F(2, 210) = .20, p = .89$
Personal Privacy * Male	17.38 (5.60)	
Personal Privacy * Female	16 00 (6.70)	
Legal Privacy Agreement * Female	18.16 (6.66)	
Legal Privacy Agreement * Male	16 25 (5 64)	
History of the Internet Control * Male	18.07 (6 62)	
History of the Internet Control * Female	17.74 (4.83)	
Gender of Target * Gender of Participant		$F(1, 210) = 06, p = .81$
Male * Male	17.90 (6.06)	
Male * Female	17 80 (6.49)	

Female * Male	16.98 (6 11)	
Female * Female	16.51 (5.64)	
Story * Gender of Target * Gender of Participant		$F(2, 210) = 34, p = 70$
Personal Privacy * Male * Male	18 20 (5 93)	
Personal Privacy * Male * Female	16.21 (5.09)	
Personal Privacy * Female * Male	16 25 (7 25)	
Personal Privacy * Female * Female	15.86 (6.49)	
Legal Privacy Agreement * Male * Male	18.29 (6.45)	
Legal Privacy Agreement * Male * Female	18.00 (7.16)	
Legal Privacy Agreement * Female * Male	17 42 (5 66)	
Legal Privacy Agreement * Female * Female	15.75 (5.65)	
History of the Internet Control * Male * Male	16.92 (6.10)	
History of the Internet Control * Male * Female	18.94 (7.04)	
History of the Internet Control * Female * Male	17 38 (6 70)	
History of the Internet Control * Female * Female	17.96 (4.49)	

*Significant at the 05 level

Note Means with same subscripts are not significantly different at least the 05 level Means with different subscripts are significantly different at least the 05 level

Table 17.

Means, Standard Deviations and F-test Statistics for Personal Identity Information, Sensitive Personal Information and Stigmatizing Information as a Function of Story and Gender

Model	Factor	Mean (SD)	F Test
Disclosure of Personal Identity Information, Sensitive Personal Information, and Stigmatizing Information			
Personal Identity Information			
	Story		$F(2, 215) = .30, p = .97$
	Personal Privacy	4 27 (1.45)	
	Legal Privacy Agreement	4 32 (1.41)	
	History of the Internet Control	4 24 (1 25)	
	Gender of Target		$F(1, 215) = .44, p = .51$
	Male	4.35 (1.46)	
	Female	4.21 (1.29)	
	Gender of Participant		$F(1, 215) = 21, p = .65$

Male	4.35 (1.42)	
Female	4.22 (1.33)	
Story * Gender of Target		F (2, 215) = .18, p = .83
Personal Privacy * Male	4.40 (1.59)	
Personal Privacy * Female	4.16 (1.32)	
Legal Privacy Agreement * Male	4.33 (1.40)	
Legal Privacy Agreement * Female	4.30 (1.44)	
History of the Internet Control * Male	4.33 (1.40)	
History of the Internet Control * Female	4.18 (1.16)	
Story * Gender of Participant		F (2, 215) = 1.30, p = .28
Personal Privacy * Male	4.38 (1.44)	
Personal Privacy * Female	4 18 (1 47)	
Legal Privacy Agreement * Male	4.55 (1.50)	
Legal Privacy Agreement * Female	4.13 (1.432)	
History of the Internet Control * Male	4 10 (1.32)	
	4.33 (1 21)	

History of the Internet Control * Female		
Gender of Target * Gender of Participant		$F(1, 215) = 19, p = 67$
Male * Male	4.51 (1.58)	
Male * Female	4 24 (1.25)	
Female * Male	4.24 (1.32)	
Female * Female	4 20 (1 33)	
Story * Gender of Target * Gender of Partıcipant		$F(2, 215) = .61, p = .55$
Personal Privacy * Male * Male	4.50 (1 61)	
Personal Privacy * Male * Female	4.25 (1.57)	
Personal Privacy * Female * Male	4.21 (1.19)	
Personal Privacy * Female * Female	4.14 (1.38)	
Legal Privacy Agreement * Male * Male	4.67 (1.53)	
Legal Privacy Agreement * Male * Female	3.83 (1 03)	
Legal Privacy Agreement * Female * Male	4.40 (1.50)	
Legal Privacy Agreement * Female * Female	4.25 (1.43)	

	History of the Internet Control * Male * Male	4.08 (1 61)	
	History of the Internet Control * Male * Female	4.53 (1.23)	
	History of the Internet Control * Female * Male	4.12 (1 11)	
	History of the Internet Control * Female * Female	4 21 (1.21)	
Sensitive Personal Information			
	Story		$F(2, 215) = 73, p = .49$
	Personal Privacy	2.91 (1.42)	
	Legal Privacy Agreement	3.04 (1 34)	
	History of the Internet Control	3 19 (1.35)	
	Gender of Target		$F(1, 215) = .15, p = .70$
	Male	3.09 (1.47)	
	Female	3 01 (1.31)	
	Gender of Participant		$F(1, 215) = .00, p = .96$
	Male	3 06 (1.44)	
	Female	3 04 (1.34)	

Story * Gender of Target		$F(2, 215) = 2\ 02, p = .14$
Personal Privacy * Male	3 14 (1 53)	
Personal Privacy * Female	2 71 (1.31)	
Legal Privacy Agreement * Male	3.20 (1.49)	
Legal Privacy Agreement * Female	2.93 (1 23)	
History of the Internet Control * Male	2 93 (1 41)	
History of the Internet Control * Female	3 37 (1 32)	
Story * Gender of Participant		$F(2, 215) = 3.69, p = .03$*
Personal Privacy * Male	2.91 (1.46)	
Personal Privacy * Female	2.91 (1.40)	
Legal Privacy Agreement * Male	3.42 (1.78)	
Legal Privacy Agreement * Female	2.73 (1.40)[a]	
History of the Internet Control * Male	2.83 (1.56)	
History of the Internet Control * Female	3 43 (1 19)[b]	
Gender of Target * Gender of Participant		$F(1, 215) = 1.75, p = .19$

Male * Male	3.23 (1.53)	
Male * Female	2.93 (1 40)	
Female * Male	2 87 (1.33)	
Female * Female	3 09 (1.31)	
Story * Gender of Target * Gender of Participant		F (2, 215) =1 28, p = .28
Personal Privacy * Male * Male	3.40 (1.57)	
Personal Privacy * Male * Female	2 76 (1.44)	
Personal Privacy * Female * Male	2 20 (.94)	
Personal Privacy * Female * Female	3.03 (1 43)	
Legal Privacy Agreement * Male * Male	3.50 (1 34)	
Legal Privacy Agreement * Male * Female	2.75 (1 66)	
Legal Privacy Agreement * Female * Male	3 33 (1.23)	
Legal Privacy Agreement * Female * Female	2.71 (1.21)	
History of the Internet Control * Male * Male	2.62 (1 66)	
History of the Internet Control * Male * Female	3 18 (1.19)	
History of the Internet Control * Female * Male		

	History of the Internet Control * Female * Female	3.00 (1.50)	
		3.59 (1.18)	
Stigmatizing Information			
	Story		$F(2, 215) = 1.70, p = .19$
	Personal Privacy	5.92 (2 96)	
	Legal Privacy Agreement	6.51 (2.78)	
	History of the Internet Control	6.79 (2.54)	
	Gender of Target		$F(1, 215) = .09, p = .76$
	Male	6.39 (2.83)	
	Female	6.41 (2.77)	
	Gender of Participant		$F(1, 215) = .78, p = 38$
	Male	6.64 (2.81)	
	Female	6.22 (2.77)	
	Story * Gender of Target		$F(2, 215) = 13, p = .88$
	Personal Privacy * Male	5 89 (2.93)	
	Personal Privacy * Female	5 95 (3.03)	

Legal Privacy Agreement * Male	6.70 (2.73)	
Legal Privacy Agreement * Female	6 37 (2.84)	
History of the Internet Control * Male	6.67 (2.82)	
History of the Internet Control * Female	6 87 (2.42)	
Story * Gender of Participant		F (2, 215) = .22, p = .81
Personal Privacy * Male	6 03 (3 14)	
Personal Privacy * Female	5.84 (2.85)	
Legal Privacy Agreement * Female	6.73 (2.60)	
Legal Privacy Agreement * Male	6.33 (2.94)	
History of the Internet Control * Male	7 23 (2 60)	
History of the Internet Control * Female	6 50 (2.54)	
Gender of Target * Gender of Participant		F (1, 215) = .4 30, p = 04*
Male * Male	6 16 (2.82)	
Male * Female	6.64 (2.85)	
Female * Male	7 17 (2 73)[a]	

Female * Female	6.00 (2.71)[b]	
Story * Gender of Target * Gender of Participant		$F(2, 215) = .01, p = .99$
Personal Privacy * Male * Male	5 60 (3.00)	
Personal Privacy * Male * Female	6 25 (2 89)	
Personal Privacy * Female * Male	6.64 (3.34)	
Personal Privacy * Female * Female	5.61 (2.86)	
Legal Privacy Agreement * Male * Male	6.44 (2.73)	
Legal Privacy Agreement * Male * Female	7.08 (2 81)	
Legal Privacy Agreement * Female * Male	7.07 (2.49)	
Legal Privacy Agreement * Female * Female	6.00 (2.98)	
History of the Internet Control * Male * Male	6.62 (2 75)	
History of the Internet Control * Male * Female	6 71 (2.98)	
History of the Internet Control * Female * Male	7.71 (2 44)	
History of the Internet Control * Female * Female	6 38 (2 31)	

*Significant at the 05 level

Note Means with same subscripts are not significantly different at least the 05 level Means with different subscripts are significantly different at least the 05 level

Table 18.

Means, Standard Deviations and F-test Statistics for Contact and View Information as a Function of Story and Gender

Disclosure within Facebook Content Areas			
Contact Information			
	Story		$F(2, 212) = 1\ 39, p = .25$
	Personal Privacy	25 (29)	
	Legal Privacy Agreement	.23 (.28)	
	History of the Internet Control	18 (.22)	
	Gender of Target		$F(1, 212) = 1.19, p = 28$
	Male	25 (.29)	
	Female	19 (.25)	
	Gender of Participant		$F(1, 212) = 4\ 01, p = .05$*

Male	.26 (29)[a]	
Female	19 (.25)[b]	
Story * Gender of Target		F (2, 212) = 3 93, p = .02*
Personal Privacy * Male	34 (.30)[a]	
Personal Privacy * Female	.17 (26)[b]	
Legal Privacy Agreement * Male	21 (.30)	
Legal Privacy Agreement * Female	.24 (27)	
History of the Internet Control * Male	.18 (.23)	
History of the Internet Control * Female	18 (22)	
Story * Gender of Participant		F (2, 212) = 3.55, p = .03*
Personal Privacy * Male	.31 (.28)[a]	
Personal Privacy * Female	.20 (.29)	
Legal Privacy Agreement * Male	.31 (.32)[a]	
Legal Privacy Agreement * Female	.16 (.23)	
History of the Internet Control * Male	.14 (.23)[b]	
	.21 (.22)	

History of the Internet Control * Female		
Gender of Target * Gender of Participant		$F(1, 212) = 5.01, p = 03$*.
Male * Male	.33 (.31)[a]	
Male * Female	.17 (.23)[b]	
Female * Male	19 (24)	
Female * Female	.20 (25)	
Story * Gender of Target * Gender of Participant		$F(2, 212) = .39, p = 68$
Personal Privacy * Male * Male	43 (.27)	
Personal Privacy * Male * Female	23 (.32)	
Personal Privacy * Female * Male	14 (.22)	
Personal Privacy * Female * Female	.18 (.28)	
Legal Privacy Agreement * Male * Male	.31 (.33)	
Legal Privacy Agreement * Male * Female	.06 (.13)	
Legal Privacy Agreement * Female * Male	.31 (31)	
Legal Privacy Agreement * Female * Female	20 (.25)	

	History of the Internet Control * Male * Male	.18 (.29)	
	History of the Internet Control * Male * Female	.19 (.17)	
	History of the Internet Control * Female * Male	.12 (.16)	
	History of the Internet Control * Female * Female	.21 (.24)	
View Information			
	Story		$F(2, 212) = .82, p = .44$
	Personal Privacy	.40 (.43)	
	Legal Privacy Agreement	.46 (.47)	
	History of the Internet Control	.51 (.44)	
	Gender of Target		$F(1, 212) = 33, p = 57$
	Male	.45 (.44)	
	Female	.45 (.46)	
	Gender of Participant		$F(1, 212) = 1.81, p = .18$
	Male	51 (.45)	
	Female	.41 (.45)	
	Story * Gender of Target		$F(2, 212) = 1.35, p = .26$

Personal Privacy * Male	.39 (.46)	
Personal Privacy * Female	.40 (.43)	
Legal Privacy Agreement * Male	53 (47)	
Legal Privacy Agreement * Female	41 (.46)	
History of the Internet Control * Male	43 (44)	
History of the Internet Control * Female	56 (.44)	
Story * Gender of Participant		$F(2, 212) = .00, p = 99$
Personal Privacy * Male	44 (.46)	
Personal Privacy * Female	.36 (.44)	
Legal Privacy Agreement * Male	53 (47)	
Legal Privacy Agreement * Female	.40 (.46)	
History of the Internet Control * Male	.57(.43)	
History of the Internet Control * Female	.47 (.45)	
Gender of Target * Gender of Participant		$F(1, 212) = 4.13, p = 04$*
Male * Male	.43 (45)	

Male * Female	.47 (47)	
Female * Male	60 (.45)a	
Female * Female	.38 (.43)b	
Story * Gender of Target * Gender of Participant		F (2, 212) = .08, p = .92
Personal Privacy * Male * Male	.38 (.46)	
Personal Privacy * Male * Female	.41 (.49)	
Personal Privacy * Female * Male	.54 (.46)	
Personal Privacy * Female * Female	.34 (41)	
Legal Privacy Agreement * Male * Male	.53 (.50)	
Legal Privacy Agreement * Male * Female	54 (.47)	
Legal Privacy Agreement * Female * Male	.54 (.50)	
Legal Privacy Agreement * Female * Female	.34 (.43)	
History of the Internet Control * Male * Male	.39 (42)	
History of the Internet Control * Male * Female	.47 (.46)	
History of the Internet Control * Female * Male	71 (.40)	
History of the Internet Control * Female * Female	.46 (45)	

*Significant at the .05 level

Note *Means with same subscripts are not significantly different at least the 05 level Means with different subscripts are significantly different at least the 05 level*

Table 19.

Factor Loadings for Exploratory Factor Analysis with Varimax Rotation of the Attitudes towards Computers Scale.

Item	Factor 1
In general, how at ease do you feel about using computers?	**.94**
In general, how comfortable do you feel about using computers?	**.96**
In general, how enthusiastic do you feel about using computers?	**.82**

Table 20.

Factor Loadings for Exploratory Factor Analysis with Varimax Rotation of the Concerns Subscale

Item	Factor	
	1	2
Please rate how concerned you are about each item when online:		
Viruses	.26	**.85**
Spam	.24	**.81**
Spyware	.30	**.86**
Hackers	**.72**	.50
Unauthorized access to personal information	**.80**	.41
Security	**.69**	.53
Identity Theft	**.87**	.24
"Online Stalkers"	**.81**	.12

Table 21.

Factor Loadings for Exploratory Factor Analysis with Varimax Rotation of the Strategy Use Subscale

Item	Factor		
	1	2	3
For each of the following, please indicate the degree to which you have used that strategy to protect your privacy online.			
1. Enabled Firewalls.	**.85**	10	.12
2. Installed Antivirus software.	**.85**	.12	-.05
3. Been extra careful about the kinds of information you submit online.	.29	**.74**	.02
4. Used a nickname, fake name or false information pertaining to your true identity.	-.02	**.71**	.03
5. Enabled strict privacy settings when using personal websites.	.14	**.71**	.25
6. Changed passwords frequently or used a strongly encrypted password.	.04	.36	**.69**
7. Enabled parental controls over Internet use.	.01	.17	**.62**
8. Password protected your computer log-in.	.25	-.26	**.69**
9. Installed spyware or malware.	**.73**	.11	.21

Table 22.

Factor Loadings for Exploratory Factor Analysis with Varimax Rotation of the Facebook Usage Scale

Item	Factor				
	1	2	3	4	5
How private are the things you've included in your Facebook profile? ("private" means either personal or confidential)	**.45**	.23	-.16	-.55	-.18
How often have you considered whether something was too personal to include in your profile?	.16	**.64**	.24	-.08	.33
In general, when you post things about people you know personally in your profile: do you ask them permission to do so?	**.51**	-.02	.34	-.47	.09
In general, when you post things about people you know personally in your profile: do you reveal their names?	**.62**	-.25	.07	-.33	.12
In general, when you post things about companies/products/employers in your Facebook profile: do you ask them permission to do so?	**.67**	-.20	28	.29	-.08
In general, when you post things about companies/products/employers in your Facebook profile: do you reveal their names	**.62**	-.37	.32	40	-.09
How well do you feel you know your profile's audience?	-.04	-.07	**.54**	.04	-.16
If you were aware of all the people who look at your Facebook profile, how likely is it that you would become more careful about what you write?	.19	**.56**	.16	.15	-.25
How often do you written highly personal things in your profile?	**.57**	-.18	-.40	.01	.28
How often have you gotten in trouble for anything you posted in your profile?	**.42**	.06	-.49	.25	.31
Are you surprised when someone you meet in person says they have seen/looked at your Facebook profile?	**.43**	.29	-.26	.27	-.27
Does it bother you that the things you post in your profile will be available online for a long time?	.30	**.62**	-.10	.07	-.34

How liable do you think you are for the things you post in your profile?	-.04	.42	.30	.20	**.63**

Table 23.

Factor Loadings for Exploratory Factor Analysis with Varimax Rotation of the Facebook Privacy Settings Behaviours Scale.

Item	Factor 1
How familiar are you with Facebook privacy settings?	**.83**
How often have you employed privacy settings yourself?	**.89**
How often have you advised others to employ their privacy settings?	**.80**

Table 24.

Factor Loadings for Exploratory Factor Analysis with Varimax Rotation of the Virtual Other Scale.

Item	Factor			
	1	2	3	4
When you post personally revealing information in your profile, who are you thinking about?				
Myself	.46	**.54**	.10	.02
No one	-.18	-.09	.35	**.87**
Friends	.49	**.65**	.16	-.00
Family	**.61**	.12	.31	-.14
Business Associates	**.71**	-.50	.33	-.05
Employer	**.74**	-.50	.26	-.10
Partners	**.61**	.47	.09	.18
Instructors	**.72**	-.45	.10	-.02
Acquaintances	**.58**	.17	-.26	-.19
E-Romantic Partners	**.58**	.33	.05	.08
Strangers	**.69**	-.19	- 48	.19
Anyone	**.55**	-.11	-.62	.32

Table 25.

Overview of Measures within Each of the Seven Grouping Categories Used in the Privacy Setting Analyses.

Group	Individual Measures	Number of Measures in Group
Attitudes Towards Computers	Positive Attitudes Towards Computers	1
Online Privacy Attitudes	Concern: Virus Concern: Entity Online Privacy Attitudes	3
Online Privacy Behaviours	Online Privacy Behaviours: General Caution Online Privacy Behaviours: Technical Protection Software Use Strategy Privacy Strategy	4
Personality	Public Self-Consciousness Private Self-Consciousness Extraversion Agreeableness Conscientiousness Emotional Stability Openness	7
Disclosure	Self Disclosure Degree of Disclosure Consideration Degree of Disclosure	3
Social Desirability	BIDR: Impression Management BIDR: Self Deceptive Enhancement	2
Virtual Other	VIRTUAL OTHER: Myself/Friends VIRTUAL OTHER: Other Referents	2

Table 26.

Means, Standard Deviations and F-test Statistics for Overall Disclosure as a Function of Context Condition and Gender

Model	Factor	Mean (SD)	F Test
Overall Disclosure			
	Context		$F(1, 214) = 22\ 51, p < 001$*
	Paper-and-Pencil	18.72(6.14)[a]	
	Online	15.19(5.20)[b]	
	Gender of Participant		$F(1, 214) = 1\ 01,\ p = .32$
	Male	17.85 (6.23)	
	Female	16.67 (5.79)	
	Gender of Target		$F(1, 214) = .30, p = .59$
	Male	17.47 (6.07)	
	Female	16.96 (5.96)	
	Context * Gender of Participant		$F(1, 214) = .10, p = .75$
	Paper-and-Pencil * Male	19 14 (6.25)	
	Paper-and-Pencil * Female	18.45 (6.10)	

Online * Female	15 64 (5.36)	
Online * Male	14.79 (5.07)	
Context * Gender of Target		$F(1, 214) = .02, p = 89$
Paper-and-Pencil * Male	19.47 (6.71)	
Paper-and-Pencil * Female	18.13 (5.63)	
Online * Male	15.63 (4.73)	
Online * Female	14.89 (5 52)	
Gender of Participant * Gender of Target		$F(1, 214) = 3\ 26, p = 07$
Male * Male	17.90 (6.01)	
Male * Female	17.80 (6.49)	
Female * Male	16.98 (6 11)	
Female * Female	16 51 (5 64)	
Context * Gender of Target * Gender of Participant		$F(1, 214) = .04, p = .84$
Paper-and-Pencil * Male * Male	18.94 (6.49)	

Paper-and-Pencil * Male * Female	20.47 (7 18)
Paper-and-Pencıl * Female * Male	19.69 (5.71)
Paper-and-Pencıl * Female * Female	17.77 (5.60)
Online * Male * Male	15.21 (3.72)
Online * Male * Female	15 85 (5.25)
Online * Female * Male	15.84 (6 00)
Onlıne * Female * Female	13.73 (4.75)

*Signıficant at the .001 level

Note Means wıth same subscripts are not sıgnificantly dıfferent at least the 05 level Means wıth dıfferent subscripts are sıgnificantly dıfferent at least the 05 level

Table 27.

Means, Standard Deviations and F-test Statistics for Personal Identity Information, Sensitive Personal Information and Stigmatizing Information as a Function Context Condition and Gender

Model	Factor	Mean (SD)	F Test
Disclosure of Personal Identity Information, Sensitive Personal Information, and Stigmatizing Information			
Personal Identity Information	Context		$F(1, 219) = 2.72, p$ .10
	Paper-and-Pencil	4.40 (1.49)	
	Online	4 12 (1.19)	
	Gender of Participant		$F(1, 219) = .15, p = .70$
	Male	4.35 (1.42)	
	Female	4.22 (1.33)	
	Gender of Target		$F(1, 219) = 1.54, p = .22$
	Male	4.35 (1.46)	
	Female	4 21 (1.30)	
	Context * Gender of Participant		$F(1, 219) = 1.39, p = .24$

Paper-and-Pencıl * Male	4.42 (1 54)	
Paper-and-Pencil * Female	4.38 (1.46)	
Onlıne * Female	4.26 (1.27)	
Online * Male	4.02 (1.14)	
Context * Gender of Target		$F(1, 219) = 04, p = .84$
Paper-and-Pencıl * Male	4.53(1 54)	
Paper-and-Pencil * Female	4.31 (1 45)	
Online * Male	4.17 (1 36)	
Onlıne * Female	4.07 (1.04)	
Gender of Participant * Gender of Target		$F(1, 219) = .02, p = 88$
Male * Male	4.45 (1.57)	
Male * Female	4 24 (1.25)	
Female * Male	4.24 (1.33)	
Female * Female	4.20 (1.33)	
Context * Gender of Target * Gender of		$F(1, 219) = 2 94, p = 09$

	Participant		
	Paper-and-Pencil * Male * Male	4.39 (1.68)	
	Paper-and-Pencil * Male * Female	4.47 (1 26)	
	Paper-and-Pencil * Female * Male	4 92 (1.04)	
	Paper-and-Pencil * Female * Female	4.26 (1.52)	
	Online * Male * Male	4.60 (1.30)	
	Online * Male * Female	4.07 (1.24)	
	Online * Female * Male	3.97 (1.36)	
	Online * Female * Female	4.07 (83)	
Sensitive Personal Information	Context		$F(1, 219) = 28.21, p < .001$*
	Paper-and-Pencil	3.48 4)[a]	
	Online	2 51 ɔ)[b]	
	Gender of Participant		$F(1, 219) = .28,\ p = .59$
	Male	3.06 (1.44)	
	Female	3.04 (1 34)	

Gender of Target		$F(1, 219) = .82, p = 37$
Male	3.09 (1.47)	
Female	3 02 (1.31)	
Context * Gender of Participant		$F(1, 219) = .25, p = .62$
Paper-and-Pencil * Male	3.47 (1 60)	
Paper-and-Pencil * Female	3.48 (1 32)	
Online * Female	2.52 (.99)	
Online * Male	2.51 (1.17)	
Context * Gender of Target		$F(1, 219) = 1.20, p = .27$
Paper-and-Pencil * Male	3 65 (1.54)	
Paper-and-Pencil * Female	3.36 (1.38)	
Online * Male	2.51 (1.16)	
Online * Female	2.52 (1 04)	
Gender of Participant * Gender of Target		$F(1, 219) = 34, p = .57$
Male * Male	3.24 (1.53)	

	Male * Female	2.87 (1.33)	
	Female * Male	2.93 (1.40)	
	Female * Female	3.09 (1.31)	
	Context * Gender of Target * Gender of Participant		$F(1, 219) = .06, p = .81$
	Paper-and-Pencil * Male * Male	3.58 (1.61)	
	Paper-and-Pencil * Male * Female	3.26 (1.59)	
	Paper-and-Pencil * Female * Male	3.85 (1.35)	
	Paper-and-Pencil * Female * Female	3.40 (1.31)	
	Online * Male * Male	2 40 (91)	
	Online * Male * Female	2.59 (1.05)	
	Online * Female * Male	2.56 (1.16)	
	Online * Female * Female	2 44 (1.04)	
Stigmatizing Information	Context		$F(1, 219) = .94, p = 34$
	Paper-and-Pencil	6.48 (2.77)	
		6.30 (2.82)	

Online		
Gender of Participant		$F(1, 219) = 29,\ p = .29$
Male	6.64 (2.81)	
Female	6.22 (2.77)	
Gender of Target		$F(1, 219) = .07, p = 79$
Male	6.39 (2.83)	
Female	6.41 (2.77)	
Context * Gender of Participant		$F(1, 219) = 3.19, p = .08$
Paper-and-Pencil * Male	6.38 (2.99)	
Paper-and-Pencil * Female	6.56 (2 61)	
Online * Female	6.98 (2.56)	
Online * Male	5.81 (2.91)	
Context * Gender of Target		$F(1, 219) = .48, p = .49$
Paper-and-Pencil * Male	6.31 (2.97)	
Paper-and-Pencil * Female	6.60 (2.65)	

Online * Male	6.47 (2.70)	
Online * Female	6 15 (2.93)	
Gender of Target * Gender of Participant		$F(1, 219) = 5.73, p = .02$*
Male * Male	6.16 (2.82)	
Male * Female	6.64 (2 85)	
Female * Male	7.17 (2 73)[a]	
Female * Female	6 00 (2.71)[b]	

Context * Gender of Target * Gender of Participant		$F(1\ 219) = 25, p = .62$
Paper-and-Pencil * Male * Male	5 92 (3 02)	
Paper-and-Pencil * Male * Female	7.26 (2.81)	
Paper-and-Pencil * Female * Male	7 38 (2.66)	
Paper-and-Pencil * Female * Female	6.38 (2.59)	
Online * Male * Male	6 73 (2.28)	
Online * Male * Female	7.11 (2 74)	
Online * Female * Male	6.34 (2.90)	
Online * Female * Female	5.19 (2.84)	

*Significant at the 05 level

Note Means with same subscripts are not significantly different at least the 05 level Means with different subscripts are significantly different at least the 05 level

Table 28.

Number of Privacy Settings as a Function of Story Condition, Gender of the Participant and Gender of the Target

Gender of the Participant	Gender of the Target	Story Condition			
		Legal privacy story	Personal privacy story	History of the internet	Total
Male	Male	1	6	3	10
	Female	2	2	4	8
Female	Male	3	1	2	6
	Female	8	11	6	25
	Total	14	20	15	49

Table 29.

Means for Relationship, Work and Contact Information as a Function of Context.

Content Area	Context Condition	Mean
Relationship Information	Paper and Pencil	.63
	Online	.55
Work Information	Paper and Pencil	.24
	Online	.08
Contact Information	Paper and Pencil	.30
	Online	.11

Table 30.

Number of Privacy Settings as a Function of Context Condition, Gender of the Participant and Gender of the Target

Gender of the Participant	Gender of the Target	Context Condition		
		Paper and Pencil	Online	Total
Male	Male	8	2	10
	Female	7	2	9
Female	Male	3	3	6
	Female	21	3	24
	Total	39	10	49

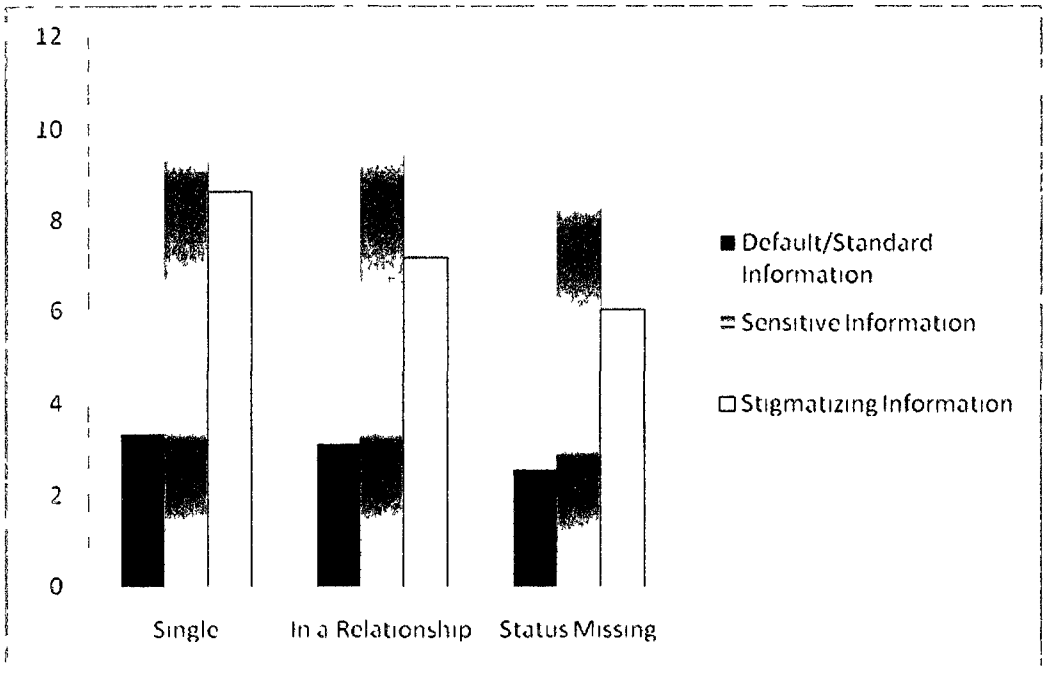


Figure 1 Presence of default/standard information, sensitive personal information, and potentially stigmatizing information as a function of relationship status (single, in a relationship and status not indicated/missing)

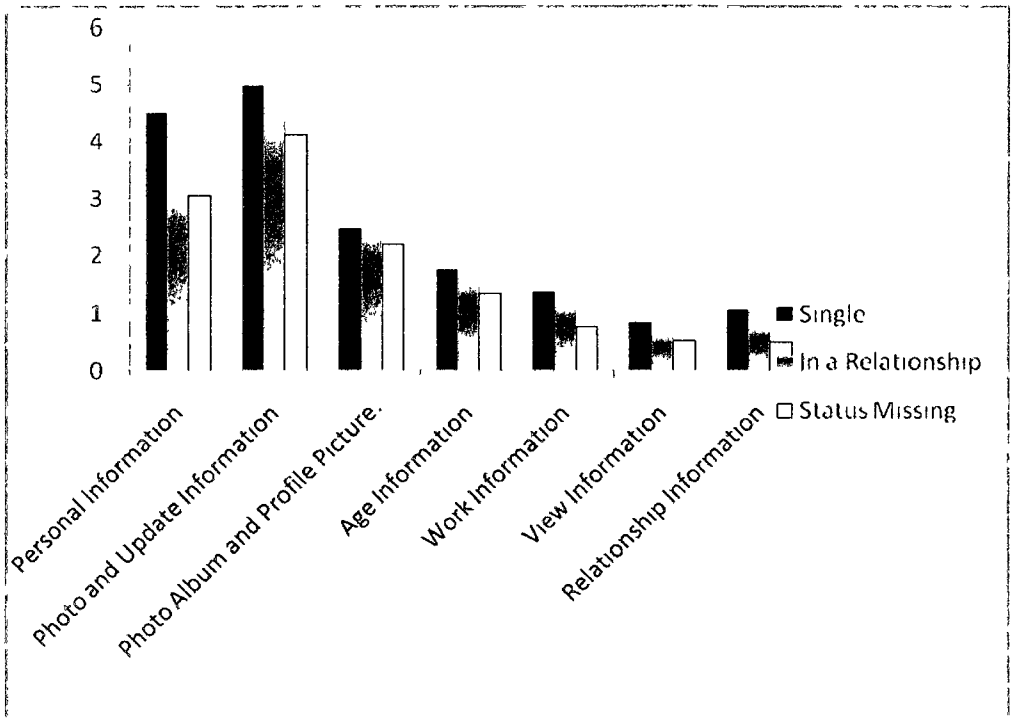


Figure 2 Presence of personal information, photo and update, Album and Profile Picture information, age information, work information, view information, and relationship information as a function of relationship status (single, in a relationship and status not indicated/missing)

Appendices

Appendix A. Glossary of Facebook Terms

About Me/Bio	Users can display personal details about themselves. For example, I love hot chocolate, I am the eldest of 3 children.
Account	A Facebook account is the sum total of all the information a user owns on Facebook, including the login and password information, the profile, the privacy settings, etc.
Activities	Users can name any activity they like to do. For example, watching television, student council, playing cards, travelling, cooking, etc. Common and/or popular activities are often depicted with a picture icon next to the activity. For example, the cooking activity is depicted with a plate of food.
Address	Users can provide their street address (e.g. house/building number and street name) in the *Contact Information* section of their profiles.
Advanced Wall	The advanced wall is similar to a bulletin board where users can display information. For example, messages to other users, large graphics, photos or videos etc.
Applications	Any additional features that are not default to Facebook. For example, Scrabulous is an application that allows users to play an online word game (Scrabble) with other users signed into Facebook.
Birthday	Users can display a "Birthday" that refers to the user's birth day, month and year.
Birth date	"Birth date" refers to the day and month that the user was born. For example, May 22.
Birth year	"Birth year" refers to the year in which the user was born. For example, 1980.
Chat	A Facebook feature that allows users to send and receive instant messages with friends who are also logged into Facebook.

College/University	Users can indicate the university/college they attended or are currently attending in the Education and Work section of their profiles. Next to "With" users can indicate other people they attended the college/university with. Once a college/university is indicated the school logo will automatically appear. Below each entered college/university, users can click on "Add a Class" to include additional institutions they have attended or are attending.
Comment	When viewing a friend's content (like a photo or note), users can leave a comment, or written observation, on that content.
Concentration	Users can indicate their discipline or area of interest (e.g. biology) in the Education and Work section of their profiles
Courses	Users can indicate any courses they took throughout their education within a high school, college/university or workshop setting.
Current City/Town	Users can name the city in which they live in the Contact Information section of their profiles.
Degree	Users can indicate the degree they are working on or have obtained (e.g. bachelors, masters etc…) in the Education and Work section of their profiles
Alumni	Users can indicate the college/university that they have graduated from.
Bachelors	Users can indicate that they hold a bachelor's degree.
Diploma	Users can indicate that they have earned a diploma.
Doctorate	Users can indicate that they hold a Doctorate degree.
Masters	Users can indicate that they hold a Master's degree.

Post-doctorate	Users can indicate that they hold a Post-doctorate degree.
Email Address	Users can provide email addresses in the Contact Information section of their profiles.
Employer	Users can display the name of their current or former employer. For example, Bank of Montreal
Events	Users can add a calendar-based resource to their profiles, pages and groups that lets them share news about upcoming affairs or social gatherings.
Facebook Blog	The official Facebook blog where users can find hundreds of posts on a wide range of subjects.
Facebook Username Link	Users have the option of creating a Facebook Username Link. A Facebook Username Link is a distinct Web address for your profile. When the Username is added to the URL your profile is easily accessed. For example, http://www.facebook.com is the Facebook homepage. But adding a Username such as http://www.facebook.com/appleseed.jonny would take you directly to Jonny Appleseed's personal profile. A Facebook Username can be searched on Facebook as well as some popular search engines so it is also another way for people to easily find friends.
Facebook Blog	The official Facebook blog where you will find hundreds of posts on a wide range of subjects.
Favourite Books	Users can indicate authors, series, comics, or genres of literature that they like. For example, Introduction to Psychology
Favourite Games	Users can indicate electronic games including computer games, video games, and personal console games, board games, and outdoor games they like. For example, Cranium.
Favourite Movies	Users can indicate TV shows and genres of shows that they like in the Arts and Entertainment section of their profiles. For example, Lord of the Rings.

Favourite Music	Users can indicate bands, songs, artists, or genres of music that they like in the Arts and Entertainment section of their profiles. For example, Lady Gaga.
Favourite Quotes	Users can indicate quotations and sayings that they like, believe in, or follow in the Philosophy section of their profiles. For example, "Birds of a Feather, Flock Together".
Favourite Teams	Users can indicate their favourite sports teams. For example, the Yankees.
Favourite Television	Users can indicate movies, movie series, and genres of movies that they like in the Arts and Entertainment section of their profiles. For example, Two and a Half Men.
Family	Users can display names of siblings, parents, aunts, uncles, cousins etc. If the family member is signed up on Facebook, their profiles will be connected. Other users can them click on the family members name, and they will be directed to that users profile.
Former Name	"Former Name" allows the user to specify whether or not they have a former name that is different from their current name. The former name may be a maiden name or a given name used prior to conducting a formal name change.
Friend	A "friend" on Facebook is a person with whom you have a reciprocal, mutually confirmed connection. All friendships on Facebook must be initiated by one party (through a friend request) and confirmed by the second party.
Friends List	Users can display a list of friends that they have accepted or have invited as Facebook friends. This list can contain a variety of individuals such as family members, high school friends, childhood friends, college friends, acquaintances and even strangers.
Friend Request	A friend request is a request to enter into a mutual friend connection with the requestee on Facebook.
Fun Wall	The fun wall is an upgraded bulletin board where users post messages or quotes, large graphics such as photos or videos, for each other to see.
Gender	Users have the option to display their gender. For example, male or female. This is not necessarily their biological sex but which gender they identify with.

Gifts	Users can accept or give virtual tokens of appreciation that are displayed as pictorial icons. These can be playful, serious and friendly gifts. For example, a birthday cake.
Graduation Year	Users can indicate the year in which they graduated or are planning to graduate.
Group Administrator	An admin is a person who's in charge of a group. When you create a group, you are automatically listed as both an admin and the group's creator. Admins can invite people to join the group, appoint other admins, and edit group information and content. They can also remove members and other admins.
Group	A group is not a page or profile. It is a Facebook site created by bands, companies and other organizations to promote their activities. Users can join groups based around shared interests, activities, political or religious causes.
High school	Users can indicate the high school they are attending or attended in the Education and Work section of their profiles.
Hometown	"Hometown" allows the user to specify the town in which they grew up in and consider their hometown. For example, London, Ontario.
IM Screen Name	Users can provide Instant Messaging Screen names in the Contact Information section their profiles. Screen names for AIM, Google Talk, Windows Live Messenger, Skype, ICQ, Twitter, and others can be added.
Inbox	The Inbox is where all messages, updates, and notifications are stored in Facebook.
Interested in	Users have the option to display their sexual orientation in the Basic Information section of their profiles. They have the option to indicate whether they are interested in men or women, or both.
Interests	Users can name any personal interest in the Activities and Interests section of their profiles. Common and/or popular interests are depicted with a picture icon next to the activity. For example, the photography interest is depicted with a camera.
Job City/Town	Users can display the city that they work in. For example, Toronto.

Job Listed	Users can display their current jobs or jobs that they have held in the past. For example: Royal Bank. Users can also list their specific job title. For example, Banker.
Job Position	Users can display what their job position is. For example, a bank teller or a manager.
Job Time Period	Users can display how long they have worked in their current job or in former jobs. For example, March 1st, 2001 – March 14th, 2011.
Like	A feature that appears as a link next to something on Facebook that allows users to let others know they appreciate that something, whether it be a video, a comment or something else.
Limited Profile	A profile that allows only restricted access.
Looking for	"Looking for" allows the user to specify what type of relationship they are looking for. A number of relationship type options are available in a drop down box next to "looking for."
Dating	"Dating" is an option in the drop down menu next to "Looking for." It means the user is looking for a dating relationship which is a form of courtship, and may include any social activity with the aim of each assessing the other's suitability as a partner.
Friendship	"Friendship" is an option in the drop down menu next to "Looking for." It means the user is looking for a friendship.
Networking	"Networking" is an option in the drop down menu next to "Looking for." It means the user is looking to connect with people who have similar interests.
Random play	"Random play" is an option in the drop down menu next to "random play." It means the user is looking to connect with a person on a casual basis without committing to a serious relationship.
Relationship	"Relationship" is an option in the drop down menu next to "Looking for." It means the user is looking for a relationship or a state of connectedness that typically includes a romantic and emotional commitment.

Whatever I can get	"Whatever I can get" is an option in the drop down menu next to "Looking for." It means the user is looking for any type of relationship.
Market Place	The marketplace is a classified ad section posted through Facebook where users can buy and sell advertised goods within the following categories: For Sale, Housing, Jobs, and Other. Ads can be posted as either available and offered, or wanted.
Market Place Listing	A listing is an entry in the Facebook Marketplace announcing that an item is for sale or exchange.
Mini-Feed	A Mini-Feed is a list of updates detailing a user's recent activity on Facebook. Recent activity can include posting on a friend's wall, being tagged in photos and/or videos, uploading an album, submitting an RSPV to a Facebook event, etc. A Mini-Feed provides details about what has been added or removed from personal profile information (e.g. relationship status, work information, likes/dislikes). The Mini-Feed is different from a News Feed in that it centres on one individual's Facebook activity and is displayed within a user's Facebook Profile.
Neighbourhood	Users can name the neighbourhood in which they live or name the nearest major intersection to where they live.
Network	Users are able to join a Facebook network which is founded in a real-world community. For example, a user can join their high school, university, city, or company network.
News Feed	News Feeds highlight what's happening in users' social circles on Facebook. It is a constantly updating list of stories about actions a user's friends have taken.
Notes	Users can display written entries detailing personal thoughts, opinions or general comments. Notes are like mini-blogs.
Notifications	Users will receive a notifications are when a friend takes an action on them on Facebook. For example, if someone tags John in a photo, John will receive a notification.
Online	This status describes whether or not a user is logged into Facebook chat.

Page	Users can add links to pages to show friends what they care about. Only the official representative of an artist or business can create and make changes to a page.
People Who Inspire You	Users can list names of people that they find inspiring. For example, Albert Einstein.
Phone	Users can display a phone number for other users to see. For example, mobile phone number, work phone number, or home phone number.
Photo Album	Users can create online photo albums where they can pick and choose pictures and upload them to their profile.
Photos	Users can upload photos of themselves and others. One can also post any pictures not related to any person, such as one's artistic drawings, that one wishes to share with others.
Political views	Users can display "Political views" or in other words, specify their political ideology. For example, Liberal. There are two boxes, one where the user can state their orientation and the other where the user can describe their political views in words.
Profile	Users who want to share information about themselves and socialize with others can create a profile. A profile displays a user's personal information and their interactions with friends.
Posted Item	Users can display links to websites, blogs, videos etc. Posts can include anything users choose to post for others to view.
Profile Picture	Users can display a profile picture which is the main photo seen at the top of each profile. This picture is associated with the users' name. Any picture can be used as a profile picture. For example, a picture of the self, a picture with friends, a picture of animals or even an avatar. An avatar is a computer generated fictional character that is usually created by the user using graphical software. Alternatively, users can take an existing picture and use this photo or graphic to represent themselves.
Relationship Status	Users have the option to display their relationship status which is found in the Basic Information section of their profile. A number of relationship options are available in the drop down box next to "Relationship Status."
Engaged	"Engaged" is an option in the drop down menu next to "Relationship Status." indicates that the user is engaged to someone.

In a relationship	"In a relationship" is an option in the drop down menu next to "Relationship Status." indicates that the user is in a relationship with someone else. Users also have the option of including the name of the person they are in a relationship with. E.g. Johnny Appleseed is in a relationship with Jane Doe.
In an open relationship	"In an open relationship" is an option in the drop down menu next to the user's "Relationship Status." This term describes a relationship in which the participants are free to have emotional and/or physical relationships with other partners.
It's complicated	"It's complicated" is an option in the drop down menu next to "Relationship Status." This term can describe a number of different relationship situations and can be used if none of the other options best describe the user's current relationship situation.
Married	"Married" is an option in the drop down menu next to "Relationship Status." indicates that the user is married.
Single	"Single" is an option in the drop down menu next to "Relationship Status." indicates that the user is not in a relationship with anyone.
Religious views	"Religious views" allows the user to specify their religious affiliation. For example, Catholic. There are two boxes, one where the user can state their religious affiliation and the other where the user can describe their religious views in words.
Residence	Users can name a retirement residence, community residence, or university residence in which they currently live or have lived in previously.
Room	Users can name the number of their apartment/room in the building or residence in which they live.
School Mailbox	Users can indicate a school mailbox number.
Self Selected Photos	Users can choose to display/upload photos of themselves or others. These photos can include profile photos or photos to include in albums.
Size of Network	Number of members in a particular network.

Status	Status updates are a way for users to keep their friends informed about what they are thinking, what they are doing, or how they might be feeling. For example, users may post things that express their current feelings, whereabouts, or actions. An update can come in the form of posted messages for all of the users' friends to read. Friends can respond with their own comments, and also press the "Like" button to show that they enjoyed reading it.
Super Wall	An upgraded bulletin board where one gets to post comments, videos and even graffiti to friends. All posts are public.
Tag	Marking a photo or video with text that identifies the image or the person in the image.
Tagged Photos	Photos that have been uploaded by another user, and where the profile user has been identified or labelled in a photo. When someone is tagged in a photo, the mouse cursor can be pointed at a person in the photo and his/her name will show up on the screen.
Videos	Users can post links to videos that they are in or that they like. Users can "tag" their friends in videos they add much like the way users can tag their friends in photos.
Wall	A bulletin board where users post messages for each other to see. This includes any random messages, such as updating your status of what you are doing, thinking or feeling, that you want to post. Once again you can post on your own wall as well on other user's walls.
Website	Users can name their personal website (e.g. one they have created for themselves or their business) or an interest website (e.g. the website for the university they attend/work for).
Zip/Postal Code	Users can input their zip or postal code in the Contact Information section of their profiles.

Appendix B. Study 1 A-3 Checklist

	Variable Name	Variable Description
1	Facebook Username Link	Web address of the Facebook profile accessed
2	Network Searched	What network (community or university) you belong to (e.g., Toronto, ON)
3	*Size of Overall Network*	Number of members in the network
4	Status Yes/No	Update information that notifies other users of your whereabouts and actions (e.g , what you are thinking, feeling, doing etc...)
5	Gender Yes/No	Sex (e.g., male, female)
6	*male*	
7	*female*	
8	Interested in (Sexual Orientation) Yes/No	Whether you are interested in men or women
9	*men*	
10	*women*	
11	Relationship Status Yes/No	Whether you are: single, in a relationship, engaged, married, it's complicated or in an open relationship
12	*single*	
13	*in a relationship*	
14	*engaged*	
15	*married*	
16	*it's complicated*	
17	*in an open relationship*	
18	Former Name Yes/No	If you are married and changed your name, what your maiden name was
19	Looking for (Relationship Preference) Yes/No	Whether you are looking for friendship, dating, a relationship, or social networking

20	*random play*	
21	*whatever I can get*	
22	*friendship*	
23	*dating*	
24	*relationship*	
25	*networking*	
26	Birthday Yes/No	The day or month you were born
27	*Birth date*	The day you were born
28	*Birth year*	The year you were born
29	Hometown Yes/No	The town you grew up in
30	Political views Yes/No	Your political stance (e.g., liberal, conservative etc .)
31	Religious views Yes/No	Your religious stance (e.g., Catholic, Muslim etc...)
32	Mini-Feed Yes/No	Updates/list of your FACEBOOK™ activity (e.g., events you are attending, friends you have added, pictures that have been posted of you etc .)
33	Email address Yes/No	Your email
34	Mobile Phone Yes/No	Your cell phone number
35	Land Phone Yes/No	Your land line phone number
36	School Mailbox Yes/No	Your school mailbox
37	Residence Yes/No	The residence you live in
38	Room Yes/No	The residence room you live in
39	Address Yes/No	Your home address
40	Current City/Town Yes/No	The city or town you live in
41	Zip Yes/No	Your zip or postal code
42	Website Yes/No	Personal or interest website address (e.g., justudents website)
43	Activities Yes/No	Things you like to do (e.g , sports, hobbies, leisure activities etc...)

44	Interests Yes/No	Your personal interests (e.g , painting, photography)
45	Favorite Music Yes/No	Bands/songs or genres of music that you like
46	Favorite TV Shows Yes/No	TV shows/genres of shows that you like
47	Favorite Movies Yes/No	Movies that you like to watch
48	Favorite Books Yes/No	Favorite books you've read
49	Favorite Quotes Yes/No	Quotations that you enjoy
50	About Me Yes/No	Personal details about yourself (e.g., you love hot chocolate and are the eldest of 3 children)
51	College/University Yes/No	The university/college you attended or are currently attending
52	Concentration Yes/No	Your discipline or area of interest (e g., biology)
53	Degree Yes/No	What degree you are working on (e.g , bachelors etc)
54	*Diploma*	
55	*Bachelors*	
56	*Masters*	
57	*Doctorate*	
58	*Post-doctorate*	
59	*Alumni*	
60	Graduation Year Yes/No	When you graduated or are planning to graduate
61	High school Yes/No	The high school you are attending or attended
62	Courses Yes/No	Any courses you took
63	Awards Yes/No	Any awards you won
64	Job Listed (have listed at least one job) Yes/No	Who you work for (or have worked for in the past)
65	Employer Yes/No	What your job position is (or was in the past)
66	Position Yes/No	What your job duties were

67	Description Yes/No	The city in which you work(ed)
68	Job City/Town Yes/No	The time period in which you worked
69	Time Period Yes/No	An upgraded bulletin board where users post messages and large graphics for each other to see, users can add applications
70	Advanced Wall Yes/No	An upgraded bulletin board where users create drawings and post graffiti for each other to see
71	Fun Wall Yes/No	An upgraded bulletin board where users post messages and large graphics for each other to see
72	Super Wall Yes/No	
73	Wall Yes/No	A bulletin board where users post messages for each other to see
74	Profile Picture Yes/No	The main photo seen at the top of your profile (e.g., picture of yourself, friends, animals etc.)
75	*self*	
76	*activity*	
77	*friends*	
78	*relationship partner*	
79	*family*	
80	*work*	
81	*school*	
82	*animal(s)*	
83	*random picture*	
84	Photos of. . Yes/No	Users can upload photos of themselves and others
85	Tagged Photos Yes/No	Photos that have been uploaded by another user, and where the profile user has been identified or labeled in a photo
86	Self Selected Photos Yes/No	Photos that have been uploaded by the actual profile user themselves
87	Tagged Videos Yes/No	Videos that the user has been identified in and tagged by another user
88	Friends Viewable Yes/No	All the friends on your friend list
89	Can you send them a gift? Yes/No	Whether you can send a gift to the user without prior permission

90	Can you message them? Yes/No	Whether you can send a message to the user without prior permission
91	Can you poke them? Yes/No	Whether you can send a poke (like a virtual nudge to let them know you are there) to the user without prior permission
92	Applications Yes/No	Any additional features that are not default to FACEBOOK™ (e.g., scrabulous, must be added by the user by signing up for the application)
93	Photo Album(s) Yes/No	Users can create online photo albums where they can pick and choose pictures and upload them to their profile
94	Groups (joined at least one group) Yes/No	Any groups that users belong to (e.g., groups based around shared interests, activities, or anything you like)
95	Events as indicated in their mini-feed Yes/No	Any parties, get-togethers or social events you are attending
96	Gifts Yes/No	Gifts that other users have sent you
97	Posted Items Yes/No	Posted websites, blogs, videos, anything users choose to post for others to view
98	Market Place listings Yes/No	A classified ad section online where users can buy and sell advertised goods
99	Notes Yes/No	Written entries detailing personal thoughts, opinions or general comments
100	Personal Pages Yes/No	Personal web pages or links that are connected to the users profile

Appendix C. Study 2 Exposure Stories

Legal Privacy Agreement Story

Facebook's Privacy Policy (Have you ever read it?)

Facebook is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence in the Internet by promoting the use of fair information practices This privacy statement covers the site www facebook com and its directly associated domains. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

When you register with Facebook, you provide us with certain personal information, such as your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information that you provide to us

When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors In addition, we store certain information from your browser using "cookies " A cookie is a piece of data stored on the user's computer tied to information about the user We use session ID cookies to confirm that users are logged in These cookies terminate once the user closes the browser By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook. You can remove or block this cookie using the settings in your browser if you want to disable this convenience feature

When you use Facebook, you may set up your personal profile, form relationships, send messages, perform searches and queries, form groups, set up events, add applications, and transmit information through various channels. We collect this information so that we can provide you the service and offer personalized features When you update information, we usually keep a backup copy of the prior version for a reasonable period of time to enable reversion to the prior version of that information

You post User Content on the Site at your own risk Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable We cannot control the actions of other Users with whom you may choose to share your pages and information Therefore, we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons We are not responsible for circumvention of any privacy settings or security measures contained on the Site You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content

Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g , photo tags) in order to provide you with more useful information and a more personalized experience

By using Facebook, you are consenting to have your personal data transferred to and processed in the United States

Personal Privacy Story

Could it happen to you?

Jennifer Porter is a little freaked out

The 17-year-old is hunkered over a sheaf of papers scattered across a Tim Hortons table in Ajax, Ont., one hand flipping pages, the other twirling an oversized blue earring " That's kind of creepy," she said.

Indeed. What she's looking at is quite the biography - everything from her cellphone number, home address and a map to her work.

She sits with myriad details of her life, furnished by me, a Globe and Mail reporter, who found Ms Porter's profile on Facebook and then reconstructed her life using nothing but freely available websites, such as Google Maps and Canada411 com.

Aside from knowing where she lives, where she works and where she will soon rest her head, our investigation also turned up her home and cellphone numbers, and when she's turning 18. Oh, and pictures, too. She's shocked that someone she has never met could learn so much about her.

'It's funny because when you called, I was having dinner with my boyfriend. He asked who it was and I said I had no clue but he got my cellphone number off Facebook," she said

Canadians are embracing social-media sites online at a breakneck pace. According to the most recent data from Com Score Inc., nearly 17 million Canadians have a Facebook profile. Social networkers use these resources to help shape their identity, essentially branding themselves and sending their public image around the world But the exposure comes at a price.

While our digital footprint expands, privacy erodes. More and more, social networkers who are not obsessively careful face the prospect of identity theft, inadvertently marring their own reputation or even inviting the threat of physical harm

While social-networking sites, such as Facebook, offer varying degrees of security and privacy protection - such as restricting who can view certain parts or the entirety of their profile - many users leave the drapes open. Whether by ignorance or simply a willingness to trust their private details to the public, they leave their photos, blog postings and personal information freely available for anyone to discover with a few clicks of a mouse.

During a two month-long investigation, The Globetracked more than a dozen Canadians through their open social-networking profiles, employing only freely available Web tools to build profiles of each individual user. Here are two examples of what we found:

> There's the 23-year-old Oakville, Ont., woman who posted her home phone number on an open Facebook profile. Plug the number into Canada411.com for a reverse address search, and you'll find her home address, which you can then search on Google Maps and see she lives on a quiet suburban street near the Queen Elizabeth Way More personal,

she's "addicted" to the MTV show *The Hills,* loves Dr. Pepper and sometimes wears contact lenses.

To celebrate the end of school, a fourth-year University of Toronto student, who has a private Facebook profile, posted in public a map to his Collingwood, Ont., cottage and left his cellphone as the contact information.

History of the Internet Control Story

The Early Years of the Internet

The Internet began as ARPAnet, a U.S. Department of Defense project to create a nationwide computer network that would continue to function even if a large portion of it were destroyed in a nuclear war or natural disaster.

Although the basic applications and guidelines that make the Internet possible had existed for almost a decade, the network did not gain a public face until the 1990s. On August 6, 1991, CERN, which straddles the border between France and Switzerland, publicized the new World Wide Web project. The Web was invented by English scientist Tim Berners-Lee in 1989.

Today, several Web browsers are available for IBM, Macintosh and UNIX-based computers. And the Web is growing at a phenomenal rate. During the 1990s, it was estimated that the Internet grew by 100% per year, with a brief period of explosive growth in 1996 and 1997. As of June 30, 2008, 1.463 billion people use the Internet according to Internet World Stats.

Through keyword-driven Internet research using search engines like Yahoo! and Google, millions of people worldwide have easy, instant access to a vast and diverse amount of online information. Compared to encyclopedias and traditional libraries, the World Wide Web allows for easy access to a variety of information and data.

The Internet has made possible entirely new forms of social interaction, activities and organizing, thanks to its basic features such as widespread usability and access.

Using the Web, individuals can publish ideas and information for an extremely large audience. Anyone can find ways to publish a web page, a blog or build a website for very little initial cost.

Many individuals use "web logs" or blogs, which are largely used as online diaries. Some commercial organizations encourage staff to fill them with advice on their areas of specialization in the hope that visitors will be impressed by the expert knowledge and free information, and be attracted to the corporation as a result.

Many use the World Wide Web to access news, weather and sports reports, to plan and book holidays and to find out more about their random ideas and casual interests. Also, many use the Internet to access and download music, movies and other works for their enjoyment and relaxation.

People use chat, messaging and e-mail to make and stay in touch with friends worldwide, sometimes in the same way as some previously had pen pals. Social networking websites like MySpace, Facebook and many others like them also put and keep people in contact for their enjoyment.

Advertising on popular web pages can be lucrative, and e-commerce or the sale of products and services directly via the Web continues to grow.

Another main area of leisure on the Internet is multiplayer gaming. This form of leisure creates communities, bringing people of all ages and origins to enjoy the fast-paced world of multiplayer games. These range from MMORPG to first-person shooters, from role-playing games to online gambling. This has revolutionized the way many people interact and spend their free time on the Internet.

Appendix D. Study 2 Target Portfolio

Female Target

Sarah D. Barnes

PERMANENT:
276 Eiwo Crt. – Apt. 103
Waterloo, ONT – N2K 2M8
519-880-1694
Barnes_RIM@gmail.com

OBJECTIVE: **Programming position with an emphasis in Internet/Web technologies**

SUMMARY:
- **Three years experience implementing Internet technologies**
- **Potential Honours graduate with BSC in Computer Science**
- **Proficient with Web tools, including Java/J2EE, Cold Fusion and .NET**

EDUCATION: BSc expected with Honours in Computer Science & Psychology Minor, June 2009
University of Ottawa, Ottawa, Ontario
Current GPA of 8.95 on a 10.0 scale

Courses taken included:
Psychology

Internet/Web Development	**Advanced Systems Design**
Advanced Java Development	**Senior Project (Web Architecture)**
Object-Oriented Programming	**Object-Oriented Analysis/Design**
Internet Communications	**C/C++ Programming**

EXPERIENCE: Programmer Internship, May 2007 to September 2007
Statistics Canada, Ottawa Ontario
- **Member of New Technologies Development Group.**
- **Evaluated new technologies for implementation throughout the organization, including Java/J2EE, HTML, Cold Fusion and .NET.**
- **Assisted in designing and developing Intranet site for Corporate Communications.**
- **Refined interface to applicant tracking system used by HR department.**

Departmental Aide, May 2006 to September 2006
IT Dept., University of Ottawa, Ottawa, Ontario
- **Assisted in developing the first campus-wide Intranet application for posting course descriptions and pre-requisites.**
- **Assisted in developing course grading systems in C++ and integrated into the Registrar's office for posting of final grades.**

ACTIVITIES
- **Member, Intramural Soccer Term 2004-2008**
- **Edward C. Grace Award for Excellence in Computing, 2007**
- **Volunteer at Elementary Schools teaching computer skills 2005-2008**

Employment Application

Full Name: **Barnes** (Last) **Sarah** (First) **D** (M.I) Date: **November 15, 2008**

Address: **276 Eiwo Crt.** (Street Address) **Apt. 103** (Apartment/Unit #)

Waterloo (City) **Ontario** (Province) **N2K 2M8** (POSTAL Code)

Phone: **(519) 880-1694** E-mail Address: **Barnes_RIM@gmail.com**

Date Available: **February 1, 2009** Social Insurance No.:749 902 487 Desired Salary: **$55,000/annual**

Position Applied for. **Programming Specialist**

	YES	NO		YES	NO
Are you a Canadian citizen?	☒	☐	If no, are you authorized to work in Canada?	☐	☐
Have you ever worked for this company?	☐	☒	If so, when?		
Have you ever been convicted of a felony?	☐	☒			

If yes, explain:

High School: **Colonel By Secondary School** Address: **2381 Ogilvie Rd. Gloucester, Ontario K1J 7N4**

From: **1999** To: **2004** Did you graduate? YES ☒ NO ☐

College: **N/A** Address:

From: To: Did you graduate? YES ☐ NO ☐ Diploma:

University **University of Ottawa** Address **75 Laurier Ave. E. Ottawa, ON K1N 6N5**

s:

From:	2005	To:	2009	Did you graduate?	YES ☐	NO ☒	Degree:	Expected: BSc with Honours in Computer Science and Psychology Minor

Please list three professional references

Full Name: **Roberto Narbaitz** Relationship: **Research Supervisor**

Company: **University of Ottawa – Faculty of Engineering** Phone: **(613) 562-5800 EXT 6142**

Address: **75 Laurier Ave. E. Ottawa, Ontario. K1N 6N5**

Full Name: **Kevin Kennedy** Relationship: **Thesis Supervisor**

Company: **University of Ottawa – Faculty of Engineering** Phone: **(613) 562-5800 EXT 6133**

Address: **75 Laurier Ave. E. Ottawa, Ontario. K1N 6N5**

Full Name: **Sarah Rizk** Relationship: **Employment Supervisor**

Company: **Statstics Canada** Phone **(613) 951-8116**

Address: **100 Tunney's Pasture Driveway, Ottawa, Ontario K1A 0T6**

Company. **Statistics Canada** Phone: **(613) 951-8116**

Address: **100 Tunney's Pasture Driveway, Ottawa, Ontario** Supervisor: **Sarah Rizk**

Job Title: **Programmer Internship** Starting Salary: **$15/hour** Ending Salary: **$16.75/hour**

Responsibilities: **Evaluate new technologies, design and develop new Intranet sites**

From: **May 2007** To: **Sept 2007** Reason for Leaving: **Going back to school**

May we contact your previous supervisor for a reference? YES ☒ NO ☐

Company: **University of Ottawa, IT Department** Phone: **(613) 562-5800 EXT 3296**

Address: **75 Laurier Ave. E., Ottawa, Ontario** Supervisor: **John Butcher**

Job Title: **Departmental Aid** Starting Salary: **$12/hour** Ending Salary: **$12/hour**

Responsibilities: **Develop new Intranet applications, research new possibilities for Intranet accessibilities**

From: **May 2006** To: **Sept 2006** Reason for Leaving: **Going back to school**

May we contact your previous supervisor for a reference? YES ☒ NO ☐

Company: **Montana's Cookhouse and Saloon** Phone: **(613) 747-2744**

Address: **1750 Ogilvie Road, Gloucester, ON K1J 7P4** Supervisor **Eric Dantey**

Job Title **Waiter** Starting Salary: **$10.75/hour** Ending Salary: **$11.50/hour**

Responsibilities: **Effective and efficient customer service, problem solving and conflict resolution**

From: **July 2004** To: **May 2006** Reason for Leaving: **Acquired new employment**

May we contact your previous supervisor for a reference? YES ☒ NO ☐

[redacted]

25 THINGS ABOUT ME...

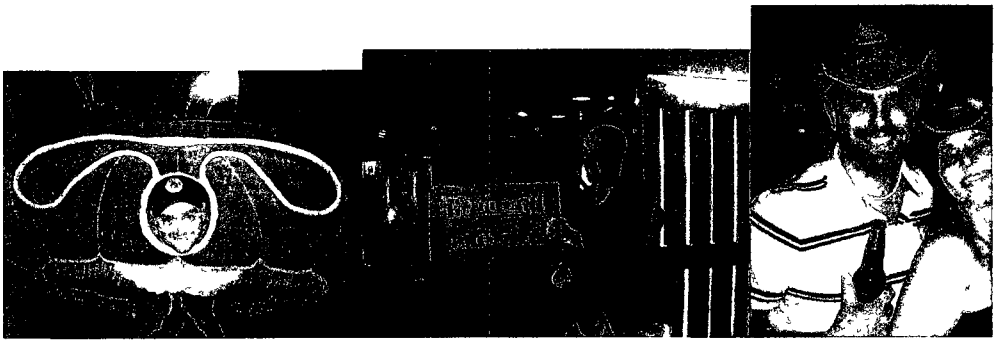
1. **My most productive hours of the day are between 11pm and 3am**
2. **I love to be active and play sports, volleyball and soccer are my two favorites ☺**
3. **If I had one wish, it would be to live on the same street as all of my friends and family, where our kids could grow up together and we could have street parties**
4. **I love the band Metric, and the movies "Zoolander" and "The Abyss"**
5. **I really enjoy online shopping**
6. **I miss living in Toronto & Ottawa, even though living in Waterloo is pretty good**
7. **I've moved 16 times**
8. **I'm turning 26 on May 22nd**
9. **I lived through a break-in**
10. **My boyfriend is my best friend and supports me no matter what I do**
11. **I believe in God and consider myself to be Catholic - but I don't go to church**
12. **I am musically challenged and absolutely admire anyone who isn't**
13. **At first glance, I may look like a nerd, but my friends think I'm the coolest person they know**
14. **I *absolutely* love the shows Arrested Development, 24 and the Office, and hope that they will make an Arrested Development movie really soon**
15. **I am really into Tae Kwon Do**
16. **I love my dog Muffin and pretty much prefer him to anyone else**
17. **I love to drive and could drive anything with wheels and a motor**
18. **Sunday Morning news shows are my favorite not because it's based on government action but because I get to see how politicians are spinning the week's news. Go Liberals!**
19. **I love the beach and I'm trained through PADI as an open-water scuba diver**
20. **I am currently feeling pretty pumped about my new YMCA membership!**
21. **I own more cereal than the grocery store**
22. **I am almost 26 and still afraid of the dark**
23. **I love getting lost.....sometimes you go places you would never have gone otherwise**
24. **I hate roast beef!**
25. **Before I went in to Computer Science & Psychology, I took a few Fine Arts courses**

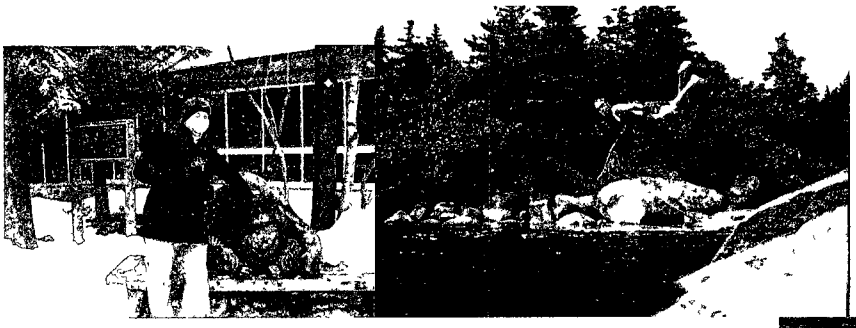
"ABOUT ME"

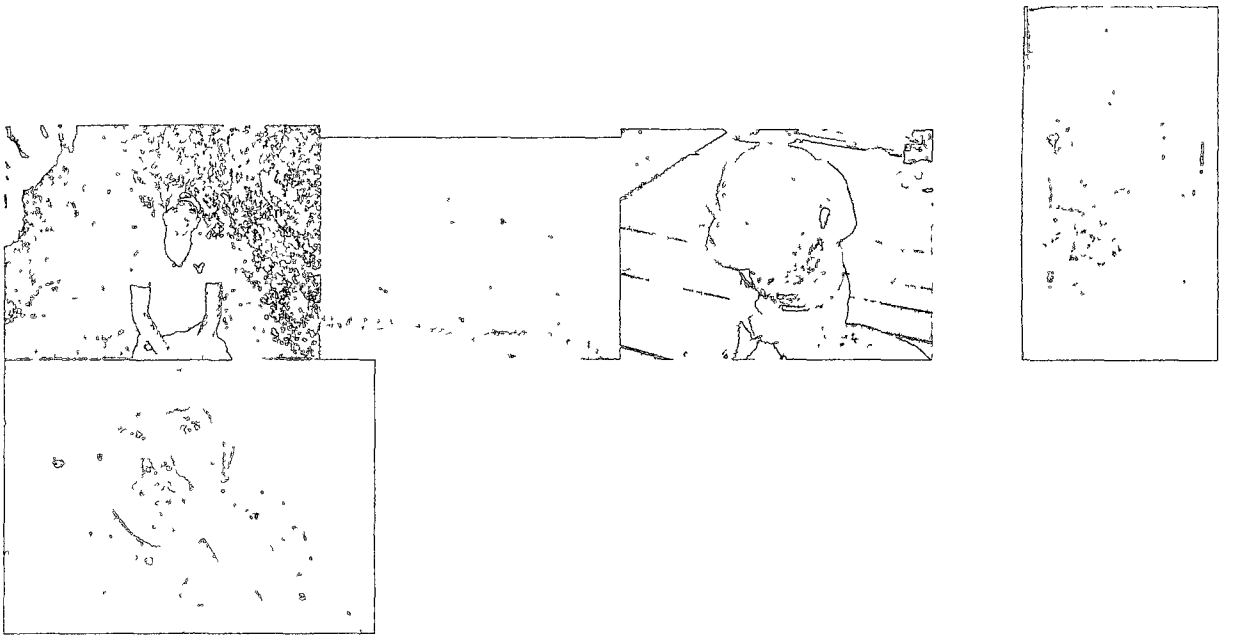
Hey there, my name is Sarah and I'm 26 years old! I am currently about to graduate from the University of Ottawa with a degree related to computer programming and will soon be heading up to Waterloo, Ontario to start work at RIM. I LOVE big cities and will miss Ottawa a lot, especially all of my friends and family, who are absolutely incredible. I love working with computers, whether it be rebuilding them or programming them – I know, such a nerd ☺ I have the best boyfriend in the entire world and he is my motivation and support for everything I do in life. I'm really scared to leave my family, friends and boyfriend to come to Waterloo, but I believe that things happen for a reason, and I feel I was meant to come to Waterloo to work, as I think I will be able to use my potential to the highest degree – guess we'll find out ☺ I LOVE being active and I'm really hoping to find some great intramural activities and/or sports to join when I get to Waterloo this spring. If you want to know anything else, just ask ☺

PHOTOS "Sarah"

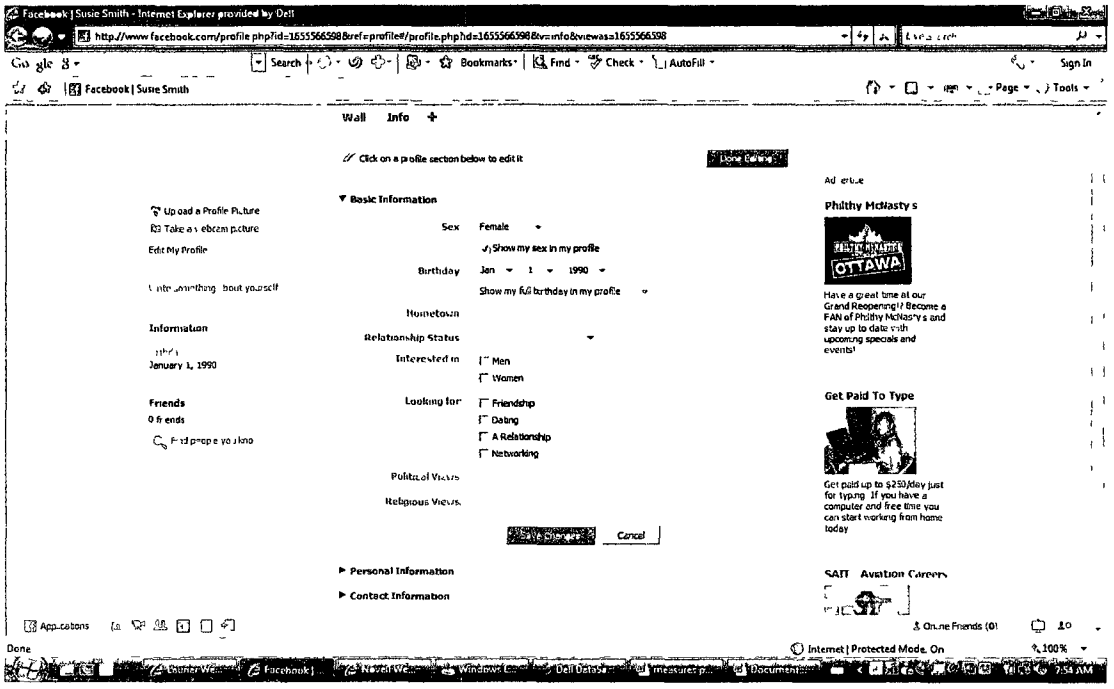
PHOTOS "Michael"

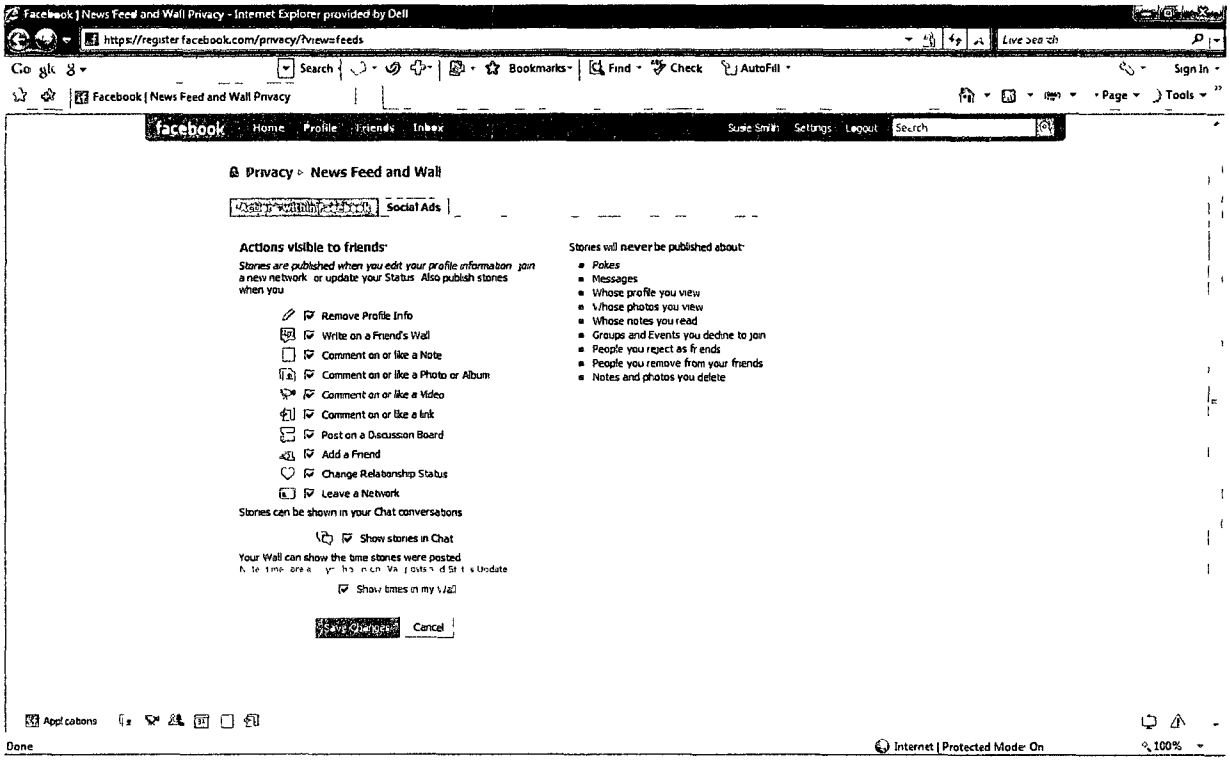






Appendix E. Study 2 Paper and Pencil Booklet




Facebook | News Feed and Wall Privacy - Internet Explorer provided by Dell
https://register.facebook.com/privacy/?views=feeds
Facebook | News Feed and Wall Privacy
facebook
Home
Profile
Friends
Inbox
Susie Smith
Settings
Logout
Search
Privacy ▸ News Feed and Wall
Social Ads
Actions visible to friends
Stories are published when you edit your profile information, join a new network, or update your Status. Also publish stories when you
Remove Profile Info
Write on a Friend's Wall
Comment on or like a Note
Comment on or like a Photo or Album
Comment on or like a Video
Comment on or like a link
Post on a Discussion Board
Add a Friend
Change Relationship Status
Leave a Network
Stories can be shown in your Chat conversations
Show stories in Chat
Your Wall can show the time stories were posted
Show times in my Wall
Cancel
Stories will never be published about
Pokes
Messages
Whose profile you view
Whose photos you view
Whose notes you read
Groups and Events you decline to join
People you reject as friends
People you remove from your friends
Notes and photos you delete
Applications
Done
Internet | Protected Mode: On
100%

Appendix F. Study 2 Privacy Settings Booklet

How to Use Privacy Settings in Facebook: Overview

What are privacy settings?

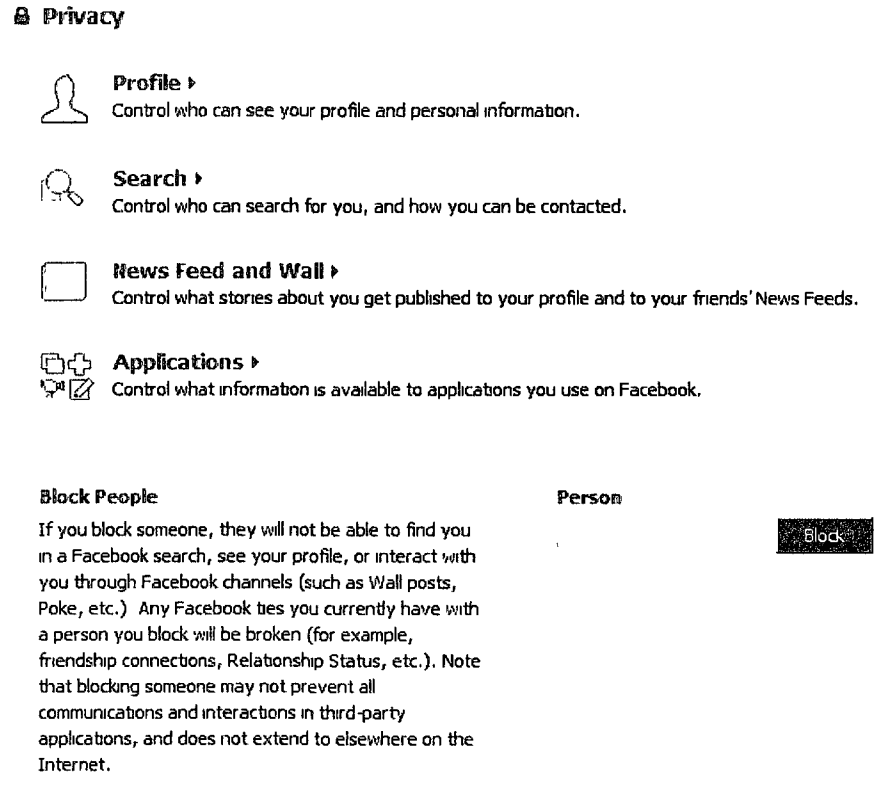
You can choose to limit who can see information presented in your profile by accessing the privacy settings. To find these, go to the top right hand tool bar and click on settings, and then click on privacy settings.

There are a variety of things you can do with the settings, for example, you can control who sees your profile and profile information. You can also control who can search for you and who can contact you. In addition, you can control what information gets published about you on Facebook (e.g., News feed stories that track your activity), and whether photos of you that you personally upload or that other users upload are visible.

How do I select/create privacy settings?

You can click on any of the four privacy setting categories (i.e., profile, search, news feed and wall, and applications). In addition, you can choose to block certain people from having the ability to search for your profile on Facebook by typing in their name under the "person" box and clicking "block". Once you've selected a category, to return to the main privacy page, simply click on the privacy heading at the top. Whenever you make changes to your settings, BE SURE TO SAVE CHANGES!!!

Here is what this page looks like:



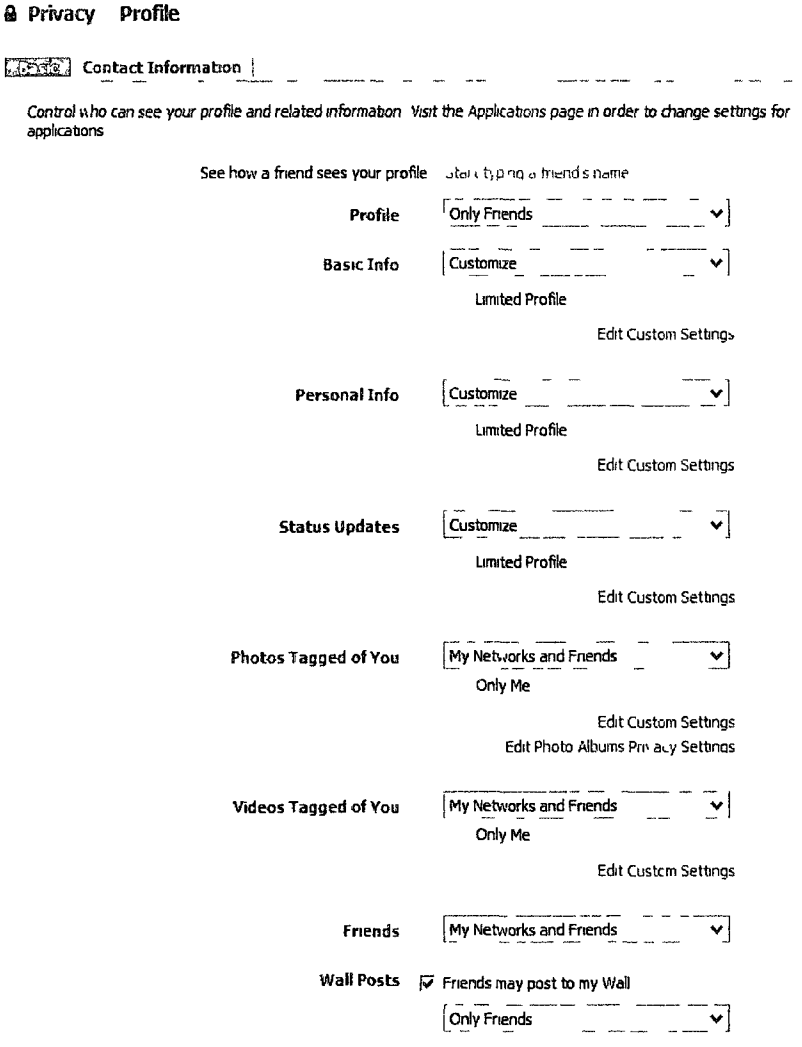
Can you walk me through privacy settings step by step?

PROFILE PRIVACY: Basic

If you click on Profile, if will bring you to a screen that has two tabs at the top (basic and contact information).

By clicking on the "basic" tab, you will be given options that allow you to set limits on who can see your profile and which information is visible to other users. This is where you can limit who sees what.

You can choose to only allow friends, friends of friends, anyone in specific networks you are a part of and their friends, or all of the networks you are a part of to see your information. By clicking on the drop down menu, you can choose who sees what for each of the components of basic profile information (e.g., photos, status updates, friends etc...) The most stringent setting is either only friends or only me (depending on the information). Here is what this page looks like:



Appendix G. Study 2 Questionnaire

Demographics

How old are you? _____

Are you? Male Female Other

What is your current relationship status?
Single
In a relationship
Married
Engaged
Divorced
In a common-law relationship

SECTION 2

Attitudes Towards Computers

Please indicate the response that best describes you.
1(not at all) 2 3 4 5 6 7(very much)

1. In general, how at ease do you feel about using computers?
2. In general, how comfortable do you feel about using computers?
3. In general, how enthusiastic do you feel about using computers?

Computer Use

How many hours do you spend per week using the computer for: (Please fill in your response with hrs/week).
Internet use _____
Recreation (e.g., games, connecting with friends, communication, shopping, banking)_____
Work/School (e.g., word processing, research, writing papers)_____

Facebook Usage Scale.

1. How private are the things you've included in your Facebook profile? ("private" means either personal or confidential)
1 (not at all) 5 (extremely)

2. How often have you considered whether something was too personal to include in your profile?
1 (not at all) 5 (extremely)

3. In general, when you post things about people you know personally in your profile:
1(never) 5 (always)
4. In general, when you post things about companies/products/employers in your Facebook profile:
1(never) 5 (always)
5. How well do you feel you know your profile's audience?
1(not at all) 5(extremely well)
6. If you were aware of all the people who look at your Facebook profile, how likely is it that you would become more careful about what you write?
1(not at all likely) 5(very likely)
7. How often do you written highly personal things in your profile?
1(never 5(all the time)
8. How often have you gotten in trouble for anything you posted in your profile?
1(never 5(all the time)
9.Are you surprised when someone you meet in person says they have seen/looked at your Facebook profile?
1(not at all) 5(extremely)
10. Does it bother you that the things you post in your profile will be available online for a long time?
1(not at all) 5(extremely)
11. How liable do you think you are for the things you post in your profile?
1(not at all) 5(extremely)

Perceptions of Technology and Uses of Technology

Do you CURRENTLY have a Facebook account? YES NO
If no, have you EVER had a Facebook account and deleted it? YES NO
How familiar are you with Facebook privacy settings?
1 (not at all familiar) 4 (somewhat familiar) 7 (very familiar)
How often have you employed privacy settings yourself?
1 (never) 4 (sometimes) 7 (always)

How often have you advised others to employ their privacy settings?
1 (never) 4 (sometimes) 7 (always)
Do you identify yourself in your Facebook profile (e.g., you indicate your real name vs. using a fake name) YES NO
How long have you been an active member of Facebook?
less than 3 months /3 to 6 months/ 6 months to a year /one to two years /over two years

SECTION 3

Public Self-Consciousness

Please select the response that best describes you
1(not at all true of me) 7(absolutely true of me)
1. I worry about what people think of me.

2. I want to amount to something special in others' eyes.

3. I feel threatened easily.

4. I need reassurance.

5. I need the approval of others.

6. I am easily intimidated.

7. I am not concerned with making a good impression

8. I feel comfortable with myself.

9. I am not easily bothered by things.

10. I am not embarrassed easily.

11. I seldom feel blue.

12. I don't worry about things that have already happened.

Private Self-Consciousness

Please select the response that best describes you.
1(not at all true of me) 7(absolutely true of me)

1. I am constantly reflecting about myself.

2. I examine my motives constantly

3. I look for hidden meaning in things.

4. I try to examine myself objectively.

5. I spend time reflecting on things.

6. I like to get lost in thought.

7. I don't try to figure myself out.

8 I rarely look for a deeper meaning in things.

9 I seldom daydream

10. I seldom get lost in thought.

Self-Disclosure

Please indicate the response that best describes you.

1(not at all true of me) 2 3 4 5 6 7(absolutely true of me)

I am open about my feelings

I am open about myself to others.

I disclose my intimate thoughts.

I show my feelings.

I talk about my worries.

I am willing to talk about myself.

I don't talk a lot.

I reveal little about myself.

I bottle up my feelings.

I have little to say

I say little.

I am hard to get to know.

I keep thoughts to myself.

BIG FIVE: ***short version (TIPI) from Gosling, Rentfrow, & Swann, 2003***

Here are a number of personality traits that may or may not apply to you. Please write a number next to each statement to indicate the extent to which you agree or disagree with that statement. You should rate the extent to which the pair of traits applies to you, even if one targetistic applies more strongly than the other.
1 = Disagree strongly, 2 = Disagree moderately, 3 = Disagree a little, 4 = Neither agree nor disagree, 5 = Agree a little, 6 = Agree moderately, 7 = Agree strongly

I see myself as:

1. _____ Extraverted, enthusiastic.
2. _____ Critical, quarrelsome.
3. _____ Dependable, self-disciplined.
4. _____ Anxious, easily upset.
5. _____ Open to new experiences, complex.
6. _____ Reserved, quiet.
7. _____ Sympathetic, warm.
8. _____ Disorganized, careless.
9. _____ Calm, emotionally stable.
10. _____ Conventional, uncreative.

Internet Security Concerns and Behaviours

1. Please rate how concerned you are about each item when online.

1 (not at all concerned) 7 (very concerned)

Viruses
Spam
Spyware
Hackers
Unauthorized access to personal information
Security
Identity theft
"Online stalkers"

2 *For each of the following, please indicate the degree to which you have used that strategy to protect your privacy online.*

1 (not at all true of me) 7 (very true of me)

Enabled Firewalls
Installed Antivirus software
Been extra careful about the kinds of information you submit online
Used a nickname, fake name, or false information pertaining to your true identity
Enabled strict privacy settings when using personal websites
Changed passwords frequently or used a strongly encrypted password
Enabled parental controls over Internet use
Password protected your computer log-in
Installed spyware or malware

Online Privacy Attitudes Scale

For each of the following questions, please indicate the response that best describes you.

1. Online sites seeking information should disclose the way the data is collected, processed and used.
1 (strongly disagree) 7 (strongly agree)
2. A good online privacy policy should have wording that is clear and easy to understand
1 (strongly disagree) 7 (strongly agree)
3. It is very important to me that I am aware and knowledgeable about how my personal information will be used.
1 (strongly disagree) 7 (strongly agree)
4. Online sites should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
1 (strongly disagree) 7 (strongly agree)
5. When people give personal information to an online site for a specific reason, the site should never use the information for any other reason.
1 (strongly disagree) 7 (strongly agree)
6. Online websites should never sell the personal information in their databases to other parties.
1 (strongly disagree) 7 (strongly agree)
7. Online websites should never share personal information with other companies unless it has been authorized by the individuals who provided the information.
1 (strongly disagree) 7 (strongly agree)
8. All things considered, the internet is capable of causing serious privacy problems.
1(strongly disagree) 7 (strongly agree)
9.Compared to others I know, I am more sensitive about the way online websites handle my personal information.
1 (strongly disagree) 7 (strongly agree)

10. To me, it is very important to maintain my privacy from online websites.
1 (strongly disagree) 7 (strongly agree)
11. I believe other people are too concerned with online privacy issues.

1 (strongly disagree) 7 (strongly agree)
12. Compared with other things on my mind or other aspects of my life, personal privacy is very important to me.
1 (strongly disagree) 7 (strongly agree)
13. I am concerned about threats to my personal privacy nowadays.
1 (strongly disagree) 7 (strongly agree)
14. In general, how experienced are you with using the Internet?
1 (not at all experienced) 7 (very experienced)
15. How frequently have you personally been the victim of what you felt was an invasion of your privacy?
1 (not at all frequently) 7 (very frequently)
16. How much have you heard or read during the last year about misuse of information *collected on the internet?*
1 (not at all frequently) 7 (very frequently)

Online Privacy Behaviours Scale

Please select the most appropriate response.

1(never) 7 (all the time)

1. How often do you shred/burn your personal documents when you are disposing of them?
2. How often do you hide your bank account card PIN number when using cash machines or making purchases?
3. How often do you only register for websites that have a privacy policy?
4. How often do you read a website's privacy policy before you register/disclose your information?
5. How often do you look for a privacy certification on a website before you register/disclose your information?
6. How often do you read website license agreements/policies fully before you agree to them?
7. How often do you watch for ways to control what people send you online (such as check boxes that allow you to opt-in or opt-out of certain offers)?
8. How often do you remove cookies?
9. How often do you use a pop-up window blocker?
10. How often do you check your computer for spy ware?
11. How often do you clear your browser history?
12. How often do you block messages/emails from someone you do not want to hear from?

SECTION 4
The Virtual Other

When you post personally revealing information in your profile, who are you thinking about?

1 (not at all true of me) 7 (absolutely true of me)

Myself
No one in particular
Friends
Family
Business associates
Employer
Romantic Partners
Instructors
Acquaintances
Ex-Romantic Partners
Strangers (whoever comes across it)
Anyone

BIDR Version 6 -Form 40A

Instructions Using the scale below as a guide, write a number beside each statement to indicate how true it is.

1	2	3	4	5	6	7
not true			somewhat true			very true

1.My first impressions of people usually turn out to be right.
2. It would be hard for me to break any of my bad habits.
3. I don't care to know what other people really think of me.
4. I have not always been honest with myself.
5. I always know why I like things.
6. When my emotions are aroused, it biases my thinking.
7. Once I've made up my mind, other people can seldom change my opinion.
8. I am not a safe driver when I exceed the speed limit.
9. I am fully in control of my own fate.
10. It's hard for me to shut off a disturbing thought.
11. I never regret my decisions.
12. I sometimes lose out on things because I can't make up my mind soon enough.
13. The reason I vote is because my vote can make a difference.
14.My parents were not always fair when they punished me.
15. I am a completely rational person.
16. I rarely appreciate criticism.
17. I am very confident of my judgments
18. I have sometimes doubted my ability as a lover.

19. It's all right with me if some people happen to dislike me.
20. I don't always know the reasons why I do the things I do.
21. I sometimes tell lies if I have to.
22. I never cover up my mistakes
23. There have been occasions when I have taken advantage of someone.
24. I never swear.
25. I sometimes try to get even rather than forgive and forget.
26. I always obey laws, even if I'm unlikely to get caught.
27. I have said something bad about a friend behind his/her back.
28. When I hear people talking privately, I avoid listening.
29. I have received too much change from a salesperson without telling him or her.
30 I always declare everything at customs.
31. When I was young I sometimes stole things.
32. I have never dropped litter on the street.
33. I sometimes drive faster than the speed limit.
34. I never read sexy books or magazines.
35. I have done things that I don't tell other people about.
36. I never take things that don't belong to me.
37. I have taken sick-leave from work or school even though I wasn't really sick.
38. I have never damaged a library book or store merchandise without reporting it.
39. I have some pretty awful habits.
40. I don't gossip about other people's business.

Appendix H: Consent Form

WILFRID LAURIER UNIVERSITY
CONSENT LETTER
Research Investigators
Dr Eileen Wood (PhD), Faculty, Department of Psychology, Wilfrid Laurier University
Amanda Nosko, PhD candidate, Department of Psychology, Wilfrid Laurier University
Miranda Kenney, Undergraduate student, Department of Psychology, Wilfrid Laurier University

You are invited to participate in a research study. The purpose of this study is to learn more about people's perceptions of technology and the self

INFORMATION You will be asked to fill out an 18 scale online survey from a lab computer on campus. In particular, you will answer questions about your self views, and about technology This session takes about 45 minutes You will also be asked to read a brief statement, and then will be provided with a booklet containing another person's personal information (e.g., job application, CV, personal photos, and personal story) We will ask you to create a Facebook profile for this person using the information provided. The profile will be constructed either online (in Facebook) or in a paper-and-pencil version of Facebook. Although the study cannot be fully explained at this time, full details will be disclosed following the conclusion of the study Approximately 240 students will participate in this study. This research is being conducted by R Eileen Wood, Amanda Nosko and Miranda Kenney as part of an ongoing research program and as part of the research projects for these students.

RISKS The risks for this study are minimal. While you complete these questions about your perceptions of self and technology, you may experience a range of emotions, some of them possibly unpleasant Remember, you can withdraw from the study at any time without penalty. We emphasize that you are free to omit a response to any question you prefer not to answer If answering some of the questions about yourself makes you feel anxious or concerned even after the study, please be aware that Wilfrid Laurier University offers confidential counseling services to its students. An appointment with Counseling Services can be made either by calling (519) 884-0710 extension 2338, email 22couns@wlu ca or by dropping by their office, located in the Student Services building, across from Health Services. You may also contact Dr Eileen Wood at ewood@wlu ca or (519) 884-0710 ext 3738, or at room N2074D in the Science Building, or Amanda Nosko at nosk2123@wlu.ca or (519) 884-0710 ext 2303 or at room N2050 in the Science Building

BENEFITS Participating in this study will give you an opportunity to experience psychological research first-hand Your responses will also help researchers understand how people think about themselves and technology.

CONFIDENTIALITY Your data will be confidential and anonymous; meaning that no one but the researchers (Dr Eileen Wood, Amanda Nosko, Miranda Kenney, Linzi Williamson, Vanessa Buote, and Amy Grant) will see your responses and will have access to the data and that the information you complete will not have your name or other identifying information on it. Please note, however, that while in transmission on the internet, your survey responses may not be entirely secure, however, the information you provide cannot be traced back to you. All of the electronic data collected will be stored on a password protected computer in a locked lab in the Science building No identifying information will be present in the data, therefore ensuring complete anonymity of response Given the nature of the survey tool we are using, all entered data will be stored and automatically added to a data file and because the information you provide will be anonymous, it is important for you to withdraw participation before entering any answers if you do not wish your answers to be included in this study. The data will be kept for approximately 8 years. All paper data (including consent forms and data) will be stored by the researchers in a locked cabinet in a locked lab in the Science Building After 8 years, the paper data will be shredded and carefully disposed of by the principal researcher

COMPENSATION For participating in this study you will receive 2 credits Other ways to earn credit is the completion of a journal article review. Details can be found in the Psychology main office (N2006, second floor, Science Building) If you withdraw from the study prior to its completion, you will receive the full amount of credit

CONTACT If you have questions at any time about the study or the procedures, (or you experience adverse effects as a result of participating in this study) you may contact the researcher, Dr. Eileen Wood at ewood@wlu.ca or (519) 884-0710 ext.3738, or at room N2074D in the Science Building, or Amanda Nosko at nosk2123@wlu.ca or (519) 884-0710 ext.2303 or at room N2050 in the Science Building This project has been reviewed and approved by the University Research Ethics Board at Wilfrid Laurier University. If you feel you have not been treated according to the descriptions in this form, or your rights as a participant in research have been violated during the course of this project, you may contact Dr Bill Marr, Chair, University Research Ethics Board, Wilfrid Laurier University, (519) 884-0710, extension 2468 or email at bmarr@wlu.ca.

PARTICIPATION Your participation in this study is voluntary; you may decline to participate without penalty. If you decide to participate, you may withdraw from the study at any time without penalty and without loss of benefits to which you are otherwise entitled. You have the right to omit any question(s)/procedure(s) you choose

FEEDBACK AND PUBLICATION Results of this research may be published at conferences or in journal articles Results will be reported only in terms of aggregated group scores The results of this study will also be posted on the Study feedback board opposite of N2006 (Psychology Main Office) on October 30, 2009

CONSENT By signing this form you indicate that you have read and understand the above information, and agree to participate in this study.

Name (please print your full name): _____

Signature _____

Date _____

Researcher initials _____

Appendix I: Debriefing Letter

WILFRID LAURIER UNIVERSITY
DEBRIEFING LETTER
Research Investigators:
Dr. Eileen Wood (PhD), Faculty, Department of Psychology, Wilfrid Laurier University
Amanda Nosko, PhD candidate, Department of Psychology, Wilfrid Laurier University
Miranda Kenney, Undergraduate student, Department of Psychology, Wilfrid Laurier University

Thank you for taking part in this study! Your participation is sincerely appreciated, and we hope that you have found your experience to be interesting. The current study was three fold.

The first line of investigation looked at a variety of issues, including privacy attitudes and behaviours both in online and offline settings, self-disclosure, familiarity and comfort with technology, Facebook usage and privacy settings, and the "virtual other" (who it is that you are thinking about when posting things on Facebook)

Second, this study examined how the wording of a privacy policy impacted on what people were willing to disclose in a Facebook profile for another person. More specifically, we were interested in seeing whether a personalized privacy statement depicting an actual invasion of privacy would result in lower levels of information disclosed when compared to the commonly used privacy statements like those seen on the Facebook website In a third control condition, participants read a statement outlining the history of the internet.

Third, we wanted to know more about how the methodology impacts on the content of a profile, that is, whether the profile was completed online in an actual Facebook profile or on a comparable paper-and-pencil version, impacted on disclosure of information. In this case, we asked you to fill out a profile for either Michael or Sarah We told you that they were actual people who had submitted their information to us, but in reality, we generated all of the information about these people. This concealment was necessary so as to encourage you to carefully consider what this person might want or not want in a personal profile. If we had told you that these people did not actually exist and that all of the information was generated, you may not have been as inclined to seriously consider the ramifications of the choices you were making while constructing the profile.

This study will help us to better understand how people are using online social communication websites, and to link various factors to one another. In addition, this study could inform policy makers on ways to more effectively tailor the wording of their policies to reach as many of their users as possible, and in the most effective way Furthermore, very little is known about how people are using Facebook, and what factors are related to their perceptions of privacy and actual employment of privacy settings, and so this study will help answer some of these questions.

If you would like to learn more about self-disclosure online, please refer to the following paper:
Joinson, A.N., Paine, C., Buchanan, T., & Reips, U.D. (2008). Measuring self-disclosure online Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behaviour, 24,* 2158-2171.

Answering some of the questions about your privacy in general and online may possibly have made you feel anxious or concerned. Wilfrid Laurier University offers confidential counseling services to its students. An appointment with Counseling Services can be made either by calling (519) 884-0710 extension 2338, email 22couns@wlu.ca or by dropping by their office, located in the Student Services building, across from Health Services. You may also contact Dr. Eileen Wood at ewood@wlu ca or (519) 884-0710 ext.3738, or at room N2074D in the Science Building, or Amanda Nosko at nosk2123@wlu.ca or (519) 884-0710 ext.2303 or at room N2050 in the Science Building. This project has been reviewed and approved by the Research Ethics Board at Wilfrid Laurier University. If you feel you have not been treated according to the descriptions in this form, or your rights as a participant in research have been violated during the course of this project, you may contact Dr. Bill Marr, Chair, University Research Ethics Board, Wilfrid Laurier University, (519) 884-0710, extension 2468 or email at bmarr@wlu.ca.

For feedback about the results of the study, please check the study feedback board opposite of N2006 Study results will be posted as soon as they are available, by October 30, 2009. Thank you again for your participation!

References

Acoca, B. (2008). *Scoping paper on online identity theft* (Ministerial Background Report DSTI/CP (2007) 3/FINAL. Retrieved May 27, 2009. Available from http:// www.oecd.org/dataoecd/35/24/40644196.pdf.

Acquisti, A., & Gross, R. (2009). Predicting Social Security numbers from public data. *The Proceedings of the National Academy of Sciences, 106(27),* 10975-10980.

Altman, I. (1975). *The environment and social behavior.* Monterey, CA: Brooks/Cole.

Altman, I. (1990). *Toward a transactional perspective: A personal journey.* In I. Altman & K. Christensen (Eds.), Environment and behavior studies: Emergence of intellectual traditions. (pp. 225-255). New York: Plenum Press.

Altman, I., & Taylor, D.A. (1973). Social penetration: The development of interpersonal relationships. Oxford, England: Holt, Rinehart & Winston.

Amichai-Hamburger, Y., Wainapel, G., & Fox, S (2002). On the Internet no one knows I'm an introvert: Extroversion, introversion, and Internet interaction. *Cyberpsychology & Behavior, 5(2),* 125-128.

Antón, A.I, Earp, J.B, Bolchini, D., He, Q., Jensen, C., & Stufflebeam, W. (2003).The lack of clarity in financial privacy policies and the need for standardization. *NCSU CSC Technical Report #TR-2003-14.*

Argyle, M. (1975). Bodily communication. Oxford, England: International Universities Press.

Bartel-Sheehan, K. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviours. *Journal of Interactive Marketing, 13(4),* 24-38.

Berendt, B., Günther, O., & Spiekermann, S. (2005). *Privacy in E-Commerce· Stated Preferences vs Actual Behavior*, Proceedings from the ACM Conference, 48(4), 101-106.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13(1),* article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Bruner, J. S. (1996). *The culture of education.* Cambridge, MA: Harvard University Press.

Buchanan, T., Paine, C., Joinson, A.N., & Reips, U.D. (2007). Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology, *58(2),* 157-165.

Bucur, A., Renold, C., III, & Henke, M. (1999). How do older netcitizens compare with their younger counterparts? *CyberPsychology & Behavior, 2,* 505–513.

Buss, A.H. (1980). *Self-consciousness and social anxiety.* San Francisco: Freeman.

Butt, S., & Phillips, J. G. (2008). Personality and self reported mobile phone use. *Computers in Human Behaviour, 24(2),* 346-360.

Carnes, P.J. (2003). The anatomy of arousal: Three Internet portals. *Sexual and Relationship Therapy, 18 (3),* 309-328.

Chaikin, A.L., & Derlega, V.J. (1974). Liking for the norm-breaker in self-disclosure. *Journal of Personality, 42,* 117-129.

Child Online Protection (COP) (2010). Retrieved on June 8, 2010, from http://www.itu.int/osg/csd/cybersecurity/gca/cop/

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on

Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology and Behavior, 12 (3),* 341-345.

Cloninger R.C., Przybeck, T.R., Svrakic, D.M., & Wetzel, R.D. (1994). *The Temperament and Target Inventory (TCI)· A guide to its development and use* St. Louis, MO: Center for Psychobiology of Personality, Washington University.

Cooper, M.L., Shapiro, C.M., & Powers, A.M. (1998). Motivations for sex and sexually risky behaviour among adolescents and young adults: A functional perspective. *The Journal of Personality and Social Psychology, 75*(6), 1528-1558.

Cosmides, L. (1989). The logic of social exchange: Has natural selection shaped how humans reason? Studies with the Wason selection task. *Cognition, 31,* 187–276.

Cranor, L. F., Reagle, J., & Ackerman, M.S. (1999). *Beyond Concern· Understanding Net Users' Attitudes about Online Privacy* AT&T Labs-Research technical report. Retrieved June 10, 2010 from http://www.research.att.com/library/trs/TRs/99/99.4.

de Wit, J., Das, E., & Vet, R. (2008). What works best: Objective statistics or a personal testimonial An assessment of the persuasive effects of different types of message data on risk perception. *Health Psychology,* 27,110-115.

Derlega, V. J., & Chaikin, A.L. (1976). Norms affecting self-disclosure in men and women. *Journal of Consulting and Clinical Psychology, 44,* 376-380.

Derlega, V.J., Metts, S., Petronio, S., & Margulis, S.T. (1993). Self-disclosure. Sage series on close relationships. Thousand Oaks, CA, US: Sage Publications, Inc.

Derlega, V.J., Durham, B., Gockel, B., & Sholis, D. (1981). Sex Differences in Self

Disclosure: Effects of Topic Content, Friendship, and Partner's Sex. *Sex Roles, 7 (4),* 433-447.

Diekman, A.B., & Eagly, A.H. (2000). Stereotypes as dynamic constructs: Women and men of the past, present, and future. *Personality and Social Psychology Bulletin, 26 (10),* 1171-1188.

Dindia, K., & Allen, M. (1992). Sex differences in self-disclosure: A meta-analysis. *Psychological Bulletin, 112,* 106–124.

Dunning, D., Johnson, K., Ehrlinger, J., & Kruger, J. (2003). *Current Directions in Psychological Science, 12(3).* 83-87. doi: 10.1111/1467-8721.01235.

Erikson, E.H. (1968). *Identity: youth and crisis.* Oxford, England: Norton & Co.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12,* 1143–1168.

Fagerlin, A., Wang, C., & Ubel, P. (2005). Reducing the influence of anecdotal reasoning on people's health care decisions: is a picture worth a thousand statistics? *Medical Decision Making,* 25,398-405.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25,* 153–160.

Grubbs-Hoy, M., & Milne, G. (2010). Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. Journal of Interactive Advertising, 10 (2), 28-45.

Giffin, K. (1967). The contributions of studies of source credibility to a theory of

interpersonal trust in the communication process. *Psychological Bulletin, 68,* 104-120.

Gilligan, C. (1982). *In a different voice: Psychological theory and women's development*. Cambridge, MA: Harvard University Press.

Goffman, E. (1959). *The presentation of self in everyday life.* New York: Anchor.

Golub, Y., Baillie, M.A., & Brown, M.J. (2007). Gender differences in internet use and online relationships, *American Journal of Psychological Research, 3(1),* 72-77.

Goodstein, A. (2007). *Totally wired: What teens and tweens are really doing online* New York, NY: Macmillan, St. Martin's Griffin.

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. Jr. (2003). A very brief measure of the big-five personality domains. *Journal of Research in Personality, 37,* 504-528.

Gouldner, A. W. (1960). The Norm of Reciprocity: A Preliminary Statement. *American Sociological Review, 25,* 161-178.

Govani, T., & Pashley, H. (unpublished manuscript). Student Awareness of the Privacy Implications When Using Facebook. Retrieved June 1, 2010 from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf.

Gross, R., & Acquisti, A. (2005, November). *Information revelation and privacy in online social networks(the Facebook case)* In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, Alexandria, VA, USA, 71-80.

Hamill, R., Wilson, T., & Nisbett, R. (1980). Insensitivity to sample bias: Generalizing from atypical cases. *Journal of Personality and Social Psychology,* 39, 578-589.

Hartley, M. (2008, September). *Social Networking Comes with a Price.* Retrieved June 1, 2010 from http://www.theglobeandmail.com /news/technology/article709699.ece.

Hian, L.B., Chuan, S.L., Trevor, T.M.K., & Detenber, B.H. (2004). Getting to know you: Exploring the development of relational intimacy in computer-mediated communication. *Journal of Computer-Mediated Communication, 9.* Retrieved December 10, 2007 from http://jcmc.indiana.edu.remote.libproxy.wlu.ca/vol9/issue3/detenber.html

Henderson, S., & Gilding, M. (2004). 'I've never clicked this much with anyone in my life': Trust and hyperpersonal communication in online friendships. *New Media & Society, 6,* 487–506.

Internet World Stats: Usage and Population Statistics (2010). Retrieved May 12, 2010, From http://www.internetworldstats.com/

Jensen, C., & Potts, C. (2004). "Privacy policies as decision-making tools: an evaluation of online privacy notices" (*Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Vienna, Austria, 477.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: the role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31,* 177–192.

Joinson, A. N. (2008). *"Looking at," "Looking up" or "Keeping up with" people? Motives and uses of Facebook.* Proceedings of CHI 2008 New York: ACM.

Joinson, A.N, Reips, U.D., Buchanan, T., & Schofield, C. (2010). Privacy, trust and self

disclosure online. *Human-Computer Interaction, 25(1),* 1-24.

Jourard, S.M. (1959). Healthy personality and self-disclosure. *Mental Hygiene, 43*, 499 507.

Jourard, S. M., & Landsman, M. J. (1960). Cognition, cathexis, and the "dyadic effect" in men's self-disclosing behavior. *Merrill Palmer Quarterly,* 6, 178-186.

Kashdan, T.B., Rose, P., & Fincham, F.D. (2004). Curiosity and exploration: Facilitating positive subjective experiences and personal growth opportunities. *Journal of Personality Assessment, 82,* 291-305.

Kehoe, C., Ptikow, J., & Morton, K. (1997). *Eighth WWW User Survey*. Retrieved from http://www.cc.gatech.edu/gvu/user_surveys/survey-1007-04/.

Kida, T. (2006). *Don't believe everything you think The 6 basic mistakes we make in thinking*. Amherst, NY: Prometheus Books.

Larson, J.H., & Bell, N.J. (1988). Need for privacy and its effect upon interpersonal attraction and interaction. *Journal of Social and Clinical Psychology, 6,* 1-10.

LaRose, R., & Rifon, N. (2006). Your privacy is assured—of being invaded: Websites with and without privacy seals. *New Media and Society, 8,* 1009–1029.

Lee, D. H., Im, S., & Taylor, C. R. (2008). Voluntary self-disclosure of information on the internet: A multi-method study of the motivations and consequences of disclosing information on blogs. *Psychology & Marketing Special Issue: New Developments in E-commerce, 25,* 692–710.

Lenhart, A., & Madden, M. (2007). *Social networking websites and teens: An overview*. Pew Internet and American Life Project report.

http://www.pewinternet.org/PPF/r/198/report_display.asp

Levesque, M.J., Steciuk, M., & Ledley, C. (2002) Self-disclosure patterns among well acquainted individuals: Disclosers, confidants and unique relationships. *Social Behavior and Personality, 30,* 579-592.

Levine, T., & Donitsa-Schmidt, S. (1998). Computer use, confidence, attitudes, and knowledge: A causal analysis. *Computers in Human Behavior*, 14 (1), 125-146.

Lewis, C., & Fabos, B. (2005). Instant messaging, literacies, and social identities. *Reading Research Quarterly, 40(4),* 470-501.

Lieberman, B. (1988). Extrapremarital intercourse: Attitudes toward a neglected sexual behavior. *Journal of Sex Research, 24,*291–299.

Locke, S.D., & Gilbert, B.O. (1995). Method of psychological assessment, self disclosure, and experiential differences: A study of computer, questionnaire, and interview assessment formats. *Journal of Social Behavior & Personality, 10,* 255-263.

Madge, C., Meek, J., Wellens, J., & Hooley, T. (2009). Facebook , social integration and informal learning at university: 'It is more for socializing and talking to friends about work than for actually doing work'. *Learning, Media and Technology, 34(2),* 141-155.

Madden, M., & Lenhart, A. (2006). *Americans who are seeking romance use the internet to help them in their search, but there is still widespread public concern about the safety of online dating.* Pew Internet and American Life Project. Available from

http://www.pewinternet.org/pdfs/PIP_Online_Dating.pdf.

Mann, B. (2007). *The polite way for a man to ask someone's age* Retrieved June 1, 2009. Available from www.associatedcontant.com/article/299592/the_polite_way_for_a_man_to_ask_someons.html.

Margulis, S.T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33,* 5-21.

Marshall, N.J. (1974). Dimensions of privacy preferences. *Multivariate Behavioral Research, 9,* 255-271.

McAdams, D. P. (2001). The psychology of life stories. *Review of General Psychology. Special Issue· Autobiographical memory, 5*, 100-122.

McAdams, D. P. (1993). The stories we live by: Personal myths and the making of the self. New York, NY, US: William Morrow & Co.

McCandlish, S. (2002). *EFF'S Top 12 ways to protect your online privacy* Retrieved on June 1, 2009. Available from http://www.eff.org/wp/effs-top-12-ways-protectyour-online-privacy.

McCrae, R.R. (1992). The five-factor model: Issues and applications [Special issue]. *Journal of Personality, 60(2).*

Metzger, M. J. (2004). Privacy, trust and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9(4)* Retrieved June 20, 2005, from http://jcmc.indiana.edu/vol9/issue4/metzger.html

Messmer, E. (2007). *Study· Facebook users easy targets for identity theft.* Retrieved on June 1, 2009. Available from http://www.macworld.com/article/59488/2007/

08/Facebook.html.

Milne, G., & Culnan, M.J. (2004). Strategies for Reducing Online Privacy Risks: Why Consumers Read [Or don't Read] Online Privacy Notices. *Journal of Interactive Marketing, 18(3),* 15-29.

Moor, J.H. (1997). Toward a theory of privacy in the information age. *Computers and Society, 27,* 27-32.

Mueller, J., Wood, E., Willoughby, T., Ross, C., & Specht, J. (2008). Identifying discriminating variables between teachers who fully integrate computers and teachers with limited integration. *Computers in Education, 51(4),* 1523-1537.

Nosko, A., Wood, E., & Desmarais, S. (2007). Unsolicited online sexual material: What affects our attitudes and likelihood to search for more. *The Canadian Journal of Human Sexuality, 16 (1-2),* 1-10.

Olson, J.S., Grudin, J., & Horowitz, E. (2005). A study of preferences for sharing and privacy, in Extended Abstracts of CHI, 1985-1988, ACM.

Oshs, E. (1979). *Planned and unplanned discourse.* In T. Givon (Ed.) Syntax and semantics, 12: Discourse and syntax (pp.51-80). New York: Academic.

O'Neil, D. (2001). Analysis of internet users' level of online privacy concerns. *Social Science Computer Review. Special Issue: The Digital Imperative of Social Sciences in the New Millenium, 19(1),* 17-31.

Paine Schofield, C.B., Joinson, A.B., Buchanan, T., & Reips, U-D. (2006). *Privacy and Self Disclosure Online,* in Extended Abstracts of CHI, Montreal, April.

Paulhus, D. L. (1984). Two-component models of socially desirable responding.

Journal of Personality and Social Psychology, 46, 598-609.

Pearce, W.B. (1974). Trust in interpersonal communication. *Speech Monographs, 41,* 236-244.

Pempek, T.A., Yermolayeva, Y.A., & Calvert, S.L. (2009). College students' social networking experiences on Facebook . *Journal of Applied Developmental Psychology, 30,* 227-238.

Prins, K. S., Buunk, B. P., & VanYperen, N.W. (1993). Equity, normative disapproval, and extramarital relationships. *Journal of Social and Personal Relationships, 10,* 39–53.

Rosen, L. D., Cheever, N. A., Cummings, C., & Felt, J. (2008). The impact of emotionality and self-disclosure on online dating versus traditional dating. *Computers in Human Behavior, 24,* 2124–2157.

Ross, C., Orr, E.M., Sisic, M., Arseneault, J.M., Simmering, M.G., & Orr, R.R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behaviour, 25(2),* 578-586.

Selwyn, N. (2009) Faceworking: exploring students' education-related use of Facebook . *Learning, Media and Technology, 34 (2),* 157-174.

Schouten, A. P., Valkenburg, P. M., & Peter, J. (2007). Precursors and Underlying Processes of Adolescents' Online Self-Disclosure: Developing and Testing an "Internet-Attribute-Perception" Model. *Media Psychology, 10, 292-315*

Schlenker, B.R. (1985). *Identity and self-identification.* In B.R. Schlenker (Ed.) The self and social life (pp. 65-99). New York: McGraw Hill.

Sullivan, D. (2008, January 14). *Web 2.0 identity theft.* Message posted to http:// www.realtimewebsecurity.com/type/mt-tb.cgi/593.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). *E-privacy in 2nd generation E commerce: Privacy preferences versus actual behavior.* Proceedings of the Third ACM Conference on Electronic Commerce, Association for Computing Machinery (ACM EC'01), 38–47. New York, NY: ACM.

Spears, R., & Lea, M. (1992). *Social influence and the influence of the 'social' in computer-mediated communication.* In Lea (Ed.), Contexts of computer-mediated communication (pp. 30-65). Hertfordshire, England: Harvester Wheatsheaf.

Sproull, L., & Keisler, S. (1986). Reducing social context cues: Electronic mail in organizational communication. *Management Science, 32,* 1492-1512.

Stanovich, K. (2009). *What intelligence tests miss. The psychology of rational thought.* Yale: University Press.

Statistics, FACEBOOK™. (2008). Retrieved January 20, 2008. Available from http:// www.Facebook.com/press/info.php?statistics.

Steffensmeier, D., & Allan, E. (1996). Gender and Crime: Toward a Gendered Theory of Female Offending. *Annual Review of Sociology, 22,* 459-487.

Stutzman, F. (2006). *Our lives, our Facebooks.* Paper presented at the 26th INSNA conference, April 24–30, in Vancouver, Canada.

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior. 7(3),* 321-326.

doi:10.1089/1094931041291295.

Swickert, R.J., Hittner, J.B., Harris, J.L., & Herring, J.A. (2002). Relationships among Internet use, personality, and social support. *Computers in Human Behaviour, 18(4),* 437-451.

Tajfel, H. (1982). Social psychology of intergroup relations. *Annual Review of Psychology, 33*, 1-39.

Tavani, H. T. & Moor, J.H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *Computers and Society, 31(1),* 6–11.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38,* 1–22. doi: 10.1111/j.1467-9973.2006.00474.x

The Canadian Internet Survey (2009). Statistics Canada. Retrieved May 12, 2010, from http://www.statcan.gc.ca/cgibin/imdb/p2SV.pl?Function=getSurvey&SDDS=4432&lang=en&db=imdb&adm=8&dis=2

Thibaut, J.W., & Kelley, H.H. (1959). The social psychology of groups. Oxford, England: Wiley.

Tidwell, L. C., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research, 28*, 317–348.

Valkenburg, P. M., Schouten, A.P., & Peter, J. (2005). Adolescents' Internet-based identity experiments: An exploratory survey. *New Media and Society, 7,* 383-402.

Viégas, F.B. (2005) Bloggers' Expectations of Privacy and Accountability: An Initial Survey.

Journal of Computer-Mediated Communication, 10(3), 00.

Waring, E. M. (1987). *Self-disclosure in cognitive marital therapy.* In V. J. Derlega & J. H. Berg (Eds.), Self-disclosure. Theory, research and therapy (pp. 283-301). New York: Plenum Press.

Walther, J.B. (1992). Interpersonal effects in computer-mediated interaction. A relational perspective. *Communication Research, 19,* 52-90.

Walther, J.B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyper-personal interaction. *Communication Research, 23,* 3–44.

Wehrli, S. (2008). Personality on social network sites: An application of the five factor model. ETH Zurich Sociology Working Paper No. 7. Retrieved online December 20th, 2010 from http://repec.ethz.ch/ets/papers/wehrli_studivz_big5.pdf.

Westin, A. (1970). *Privacy and freedom.* New York: Atheneum Press.

Westin, A. (1997). *Privacy and American business study.* Retrieved online November 1, 2010 from http://shell.idt.it/pab/women.html.

WHOA (2008), *"Comparison Statistics 2000-2009,"* available at http://haltabuse.org/resources/stats/Cumulative2000-2007.pdf (accessed September 15, 2010).

Wheeless, L.R. (1978). A follow-up study of the relationships among trust, disclosure, and interpersonal solidarity. *Human Communication Research, 4,* 143-157.

Wheeless, L.R., & Grotz, J. (1977). The measurement of trust and its relationship to self disclosure. *Human Communication Research, 3,* 250-257.

Willard, N. E. (2006). *A briefing for educators: Online social networking communities*

and youth risk Center for Sage and Responsible Internet Use.

Wiley, C., & Sisson, M. (2006, November). *Ethics, accuracy and assumption: The use of Facebook by students and employers.* Paper presented at the Southwestern Ohio Council for Higher Education Special Topics Forum, Dayton, OH.

Wilson, K., Fornasier, S., & White, K.M. (2010). Psychological Predictors of Young Adults' Use of Social Networking Sites. *Cyberpsychology, Behavior, and Social Networking, 13(2),* 173-177.

Wohlwill, J. F. (1973). *The environment is not in the head!* In W. F. E. Preiser (Ed.), Environmental design research: Vol. 2. Symposia and workshops (pp. 166-181). Stroudsburg, PA: Dowden, Hutchinson & Ross.

Wood, E., Nosko, A., Desmarais, S., Ross, C., & Irvine, C. (2006). Online and traditional paper-and-pencil survey administration: Examining experimenter presence, sensitive material and long surveys. *The Canadian Journal of Human Sexuality, 15(3-4), 147-155*

World Internet Users (2010). http://www.internetworldstats.com/stats.htm.

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior, 11(6),* 763-765.

Yum, K. (2007). *Facebook says 'Thanks, Canada'.* National Post; May 18.