The Next Digital Divide:
Online Social Network Privacy

Avner Levin
Mary Foster
Bettina West
Mary Jo Nicholson
Tony Hernandez
Wendy Cukier

Research Associates: Emily Ho, Sarah Lasch and Aubrey Podolsky

Ryerson University
Ted Rogers School of Management
Privacy and Cyber Crime Institute
March 2008
Acknowledgements

This project has been funded by the Office of the Privacy Commissioner of Canada’s Contributions Program and through in-kind contributions from the Dean of the Ted Rogers School of Management at Ryerson University. We are grateful to the Privacy Commissioner and to the Dean for their support of this important research. We also wish to thank the project participants who were willing to give up their valuable time in order to advance our understanding of the policies, practices and risks of online social networks. This project would not have been completed in such a timely fashion were it not for our very able research associates, Emily Ho, Sarah Lasch and Aubrey Podolsky who worked tirelessly on this project.
Table of Contents

Executive Summary ........................................................................................................... 8

Key Findings ..................................................................................................................... 8

Recommendations to Organizations .............................................................................. 9

Recommendations to the Office of the Privacy Commissioner .................................. 9

Introduction .................................................................................................................... 10

Project Goals and Objectives ....................................................................................... 14

Methodology ................................................................................................................... 15

Phase 1: Quantitative Survey of Young Canadians ....................................................... 15

The Sample ...................................................................................................................... 15

Analytical Approach ....................................................................................................... 18

Phase 2: Organizations ................................................................................................... 19

Results of Quantitative Survey of Young Canadians ..................................................... 21

Use of the Internet and Online Tools ............................................................................ 21

Personal Information on Online Social Networks ....................................................... 24

Online Social Networks at Work ................................................................................... 26

Risk and Responsibility Scenarios ................................................................................ 29

Scenario 1: Relationship Breakup ................................................................................ 29

Scenario 2: Party Time .................................................................................................. 33

Scenario 3: False Charges ............................................................................................ 36
Scenario 4: Sick Leave ............................................................... 39
Scenario 5: Workplace Uses of Online Social Networks .............. 41
Comparison of Responsibility Assignment across Scenarios .......... 44
Sub-group Comparisons: Gender and Year of Study .................. 44
  Scenario 1: Relationship Breakup ........................................... 45
  Scenario 2: Party Time ............................................................ 47
  Scenario 3: False Charges ...................................................... 49
  Scenario 4: Sick Leave ........................................................... 50
  Scenario 5: Workplace Uses of OSNs ..................................... 52
Gender Differences Summary .................................................. 54
Open-ended Comments .......................................................... 55
  Personal Life Concerns ......................................................... 55
  Work Life Concerns ............................................................. 62
The Perspective of Organizations ............................................. 66
  Awareness and Personal Use of Online Social Networks .......... 66
  Corporate Policies and Practices ........................................... 67
  Issues and Concerns about Online Social Networks ................ 69
  Work Life / Personal Life Boundaries ..................................... 70
  Recruitment and Selection: Human Resources Use of Online Social Networks . 71
  Marketing Application of Online Social Networks .................. 72
  Potential Uses of Online Social Networks ............................. 73
Implications and Recommendations ................................................................. 74

Recommendations for Organizations ................................................................. 75

Explicit Policies ................................................................................................. 75

Internal Guidelines ............................................................................................. 76

Marketing .............................................................................................................. 76

Education and Awareness ................................................................................... 76

Recommendations for the OPC ......................................................................... 77

Public Education and Outreach .......................................................................... 77

OSNs and PIPEDA ............................................................................................... 78

Network Privacy Breaches .................................................................................. 78

Appendix A .......................................................................................................... 79

Appendix B ......................................................................................................... 93

List of Tables

Table 1: Summary of Industries and Positions ...................................................... 19
Table 2: Frequency of Issues Identified Related to Personal Life .......................... 55
Table 3: Frequency of Issues Identified Related to Work Life ............................... 62
List of Charts

Chart 1: Respondent Age .............................................................................................................................................. 16
Chart 2: Respondent Year of Study ................................................................................................................................. 16
Chart 3: Respondents by Ryerson Faculty .......................................................................................................................... 17
Chart 4: Respondents by Gender ....................................................................................................................................... 17
Chart 5: Respondent Weekly Work Hours .......................................................................................................................... 18
Chart 6: Usage of Online Tools ........................................................................................................................................... 21
Chart 7: Online Social Networks ........................................................................................................................................ 22
Chart 8: Usage of OSNs ..................................................................................................................................................... 23
Chart 9: Extent of Information included on OSNs ................................................................................................................ 24
Chart 10: Concerns about Who is Accessing OSN Information ............................................................................................ 25
Chart 11: Actions Taken to Protect Privacy ....................................................................................................................... 26
Chart 12: OSNs in the Workplace ....................................................................................................................................... 27
Chart 13: Employer Policies relating to OSN use .................................................................................................................. 28
Chart 14: Relationship Breakup Scenario: Has this Happened? ....................................................................................... 30
Chart 15: Responsibility for Adverse Social Consequences ................................................................................................. 31
Chart 16: Reactions to Posting of Damaging Material ...................................................................................................... 32
Chart 17: Party Time Scenario: Has this Happened? .......................................................................................................... 33
Chart 18: Responsibility for Embarrassing Behaviour Consequences .................................................................................. 34
Chart 19: Reactions to Posting of Embarrassing Material ................................................................................................ 35
Chart 20: False Charges Scenario: Has this Happened? ..................................................................................................... 36
Chart 21: Responsibility for Defamatory Content Consequences .......................................................................................... 37
Chart 22: Reactions to Posting of Defamatory Material ....................................................................................................... 38
Chart 23: Sick Leave Scenario: Has this Happened? .......................................................................................................... 39
Chart 24: Responsibility for Adverse Workplace Consequences .......................................................................................... 40
Chart 25: Reactions to Workplace Consequences ................................................................. 41
Chart 26: Employer Use of OSNs .......................................................................................... 42
Chart 27: Role of OSNs in the Workplace ................................................................................ 43
Chart 28: Perspectives of Responsibility ................................................................................ 44
Chart 29: Responsibility for Adverse Social Consequences by Gender ................................. 45
Chart 30: Reactions to Posting of Damaging Material by Gender .............................................. 46
Chart 31: Responsibility for Embarrassing Behaviour Consequences by Gender ...................... 47
Chart 32: Reactions to Posting of Embarrassing Material by Gender ......................................... 48
Chart 33: Responsibility for Defamatory Content Consequences by Gender ............................ 49
Chart 34: Reactions to Posting of Defamatory Material by Gender ........................................... 50
Chart 35: Responsibility for Adverse Workplace Consequences by Gender ............................. 51
Chart 36: Reactions to Workplace Consequences by Gender .................................................. 52
Chart 37: Employer Use of OSNs and Gender ......................................................................... 53
Chart 38: Role of OSNs in the Workplace and Gender .............................................................. 54
Chart 39: OSN Concerns Related to Personal Life .................................................................... 56
Chart 40: Stranger Concerns - No Explicit Access Given (37% of total) .................................... 57
Chart 41: Relationship Concerns - Access Given (32% of total) ............................................. 57
Chart 42: OSN Concerns Related to Work Life ........................................................................ 63
Executive Summary

This report provides the largest survey to-date on the usage, attitudes and perceptions of risk over 2000 young Canadians engaged in online socializing. In addition, the report provides findings, based on sixteen in-depth interviews with leading public and private sector organizations, on the use of online social networks by organizations for commercial purposes, and offers recommendations on how the risks of online socializing can be reduced and privacy be protected.

Key Findings

- Nine out of ten young Canadians socialises online regularly and frequently
- Young Canadians are largely aware of the risks of online socializing, and have attempted to control the release of their personal information online
- A new digital divide has been created between a generation of young Canadians and a generation of managers and executives for which young Canadians work
- Young Canadians have a unique perception of network privacy, according to which personal information is considered private as long as it is limited to their social network
- Organizations reject and do not recognize the notion of network privacy. Instead, they subscribe to the view that information posted online is public and deserves no protection
- Organizations do not have policies, practices or guidelines in place that explicitly govern the use of online social networks by their employees, or by the organizations themselves for marketing and for human resources purposes
- Online social networks, while benefiting greatly from the advertising revenue generated by their users’ personal information, have successfully created a public image of their business as a passive conduit, pipeline or wall, on which personal information can be displayed, and have avoided responsibility in the public mind for any harm caused to the privacy or reputation of their users
Recommendations to Organizations

- Develop an understanding of online social networks and their role in the culture and communication behaviour of young Canadians – your customers and your employees
- Develop clear rules and guidelines about the use of online social networks at work and at home based on principles that employees will accept
- Support these policies with appropriate tools and enforcement
- Do not actively seek information from online social networks for recruitment and selection processes, and if access to such information is obtained, refrain from using it
- Ensure that uses of online social networks or the information obtained from them to fulfill marketing goals and objectives are in compliance with PIPEDA

Recommendations to the Office of the Privacy Commissioner

- Explore the tools and approaches appropriate to developing a collaborative campaign targeting young Canadians to ensure that they take appropriate steps to protect their privacy on online social networks
- Work with the online social networks to develop tools or policies to ensure the protection of individual privacy
- Advocate that online social networks providers assume greater responsibility for privacy breaches, and that they provide more resources to raise awareness and educate individuals about privacy risks
- Establish mechanisms and processes to monitor and anticipate emerging trends in social networking that may jeopardize the privacy of Canadians
- Ensure that the legal and regulatory frameworks for the protection of Canadians keep pace with these developments.
Introduction

Social networking online, on services such as My Space and Facebook, has become the preferred way of communicating for many young people, outpacing e-mail in some markets. The social networking site MySpace ranks sixth in overall web traffic, with over 47 million unique US visitors each month while web traffic data for Facebook, a social networking site oriented towards university and college students, shows 15 million unique US visitors a month.\(^1\) Facebook itself claims that it has seven million Canadian users and eight million UK users.\(^2\)

Online social networks (OSNs) are a form of controlled group communications which have evolved from small scale special purpose sites to broader general purpose communications. When users sign up for social networking sites, they create a profile which may be accessible to other members of the network. Users can define the level of access and information that they provide – restricting access to a small number of friends in a limited and well-defined group – or making information more broadly available. Profiles may include a real name, or a pseudonym; contact information (email, telephone, address); birth date, photographs, hometown, religion, ethnicity, personal interests and much more. Other users can send messages asking to become a “friend” and must be accepted by the receiving party in order to establish a link which in turn provides access to their profile and information. Some of these users appear to be posting revealing, personal information with little thought or regard for either the short-term or long-term consequences.

Unfortunately, OSNs appear to pose privacy and security threats and expose many users to a variety of forms of internet crime\(^3\). Anecdotally, high profile incidents have suggested that social networking sites can expose users to social embarrassment, large scale privacy breaches,\(^4\) identity theft, harassment and other forms of victimization.\(^5\) Previous studies have suggested that OSN users have many misconceptions about threats to their security and

\(^1\) Dwyer, C. “Digital Relationships in the ‘MySpace’ Generation: Results From a Qualitative Study.” Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS), Hawaii, 2007.
\(^3\) Cukier, W. & Levin, A. “Spam and Internet Fraud”, M. Pittaro et. al, eds., Crimes of the Internet, Prentice Hall, 2008
privacy\textsuperscript{6} and that it is relatively easy to obtain confidential information from OSNs. Using relatively simply tools, researchers have exposed at least three major threats to security on Facebook in a study of US students: users disclose too much information, Facebook does not take adequate steps to protect user privacy and third parties are actively seeking out end-user information using Facebook.\textsuperscript{7}

Our current project, funded by the Office of the Privacy Commissioner, provides an opportunity to build on previous work, and explore the attitudes and perceptions of young social networking users to privacy and security as well as organizational policies on the use of social networking.

Personal information protection aims to provide members of society with autonomy or control. Policy makers proceed from the assumption that policy and practices should be developed to allow an individual, to the greatest extent possible and in balance with other legitimate interests of other individuals and society at large, control over their personal information. The phenomenon of online social networking poses a fundamental challenge to this assumption. Individuals post personal information online, often at potential personal risk, and make it available to a large audience of “friends”, seemingly without much concern over the loss of control once information has been disseminated via their social network software of choice.

There are a variety of possible explanations (not mutually exclusive) as to why online social networkers largely ignore risks related to their personal information:

**Lack of Awareness.** Online socialisers, perhaps due to demographics, are largely oblivious to the risks to which they are exposing themselves. Online social networking appears to be increasing exponentially among young individuals in their teens and twenties. The increase in networking, however, does not appear to be accompanied by an increase in the awareness of the risks posed by posting personal information online. Some of these risks, such as career risks, may be of particular importance to students who are about to enter the full-time workforce. Other risks, such as identity theft, spamming (mass commercial emailing), phishing (inserting a fraudulent link into an email to commit fraud) and pharming (diverting Internet traffic to a fraudulent website), are a common concern to all Internet users, but may be more of a threat to online socialisers due to their increased and enhanced online presence.


Perception of Risk and Behaviour among Youth. The tendency of youth (15 – 24 year olds) to engage in high risk behaviour in spite of clearly identified risks is well-established in both the crime and health literatures.\textsuperscript{8} There is also strong evidence that these same proclivities are extended to the internet.\textsuperscript{9} The literatures on crime and injury prevention suggest that given the gap between knowledge and behaviour, relying entirely on individual agency and choice may insufficiently reduce the exposure to cyber-crime, particularly where vulnerable young people are concerned. Classic integrated models of crime and injury prevention are being evolved to address new forms of threats on the internet.\textsuperscript{10} Typically these models couple educational or awareness raising activities, with a combination of technological, regulatory, economic and enforcement elements, in an effort to change behaviour.\textsuperscript{11}

Notion of Network Privacy. Online socialisers do not view their privacy and the protection of their personal information as based on the value of personal control. It appears that their expectation of privacy is shaped not by their sense of autonomy, but by their sense of reputation and dignity, and when they perceive that their privacy is being threatened, it is really their reputation, dignity, persona or online identity that is at stake. Further, their persona and therefore their sense of dignity, reputation and privacy depend on, and are a manifestation of, the network within which they participate. Individuals may present one identity or persona to their peers, another to their work colleagues, a third to their family and a fourth to their business associates. Privacy, in a sense, is two-dimensional for such online socialisers. They are concerned not only about the extent of the dissemination of their personal information (how many people know), but also about their information’s destination (who knows). We define this perception of privacy in this report as network privacy. This understanding of privacy is similar and complementary, though not identical, to recent explanations of privacy in regular social contexts, which place an emphasis on an individual’s expectation of the extent of the dissemination of their private information, rather than on whether the individual expects their private information to be disseminated at all.\textsuperscript{12}

Neither the practice of online social networking nor the associated risks is well researched in a Canadian context, although some provincial Privacy Commissioners have introduced guidelines


\textsuperscript{11} Cukier, W. & Levin, A. supra note 3.

about online social networking. 13 This report provides the OPC with detailed information on the use of OSNs by individuals and by organizations, as well as recommendations for the OPC about how policy and guidelines on the phenomenon of online social networking can continue to be developed. Organizations have reported, for example, that online information about individuals plays a role in hiring and career development decisions, without formal policies or guidelines in place. This report recommends best practices in this regard.

The following sections of the report discuss the two research phases of this project and their results. Our report offers the largest quantitative survey to-date on the use of OSNs by young Canadians, and analyzes this usage in detail. The quantitative analysis is followed by an analysis of private and public sector interviews that were conducted with both federally and non-federally regulated organizations in order to determine their policies, practices and perceptions of OSNs. We then suggest some best practices for organizations, as well as some further steps that can be taken by the OPC in order to ensure that this next digital divide, the perception of public and private on OSNs, is bridged as safely as possible.

Project Goals and Objectives

The overall goal of this report is to provide insight into the nature and scope of risk perception, motivation, awareness and concerns (both immediate and long-term) among those engaging in online socializing. Of particular interest are the attitudes of those Canadians who are entering the workforce at a time when organizations are embarking on the replacement of the generation known as the “baby-boomers”. Recruiters need to know whether these young Canadians form a distinctive demographic group in terms of their overall approach to online socializing. The Ted Rogers School of Management at Ryerson University is particularly well-positioned to conduct a research project into the risks of online social networking as perceived by young Canadians, since it has access to a sample of this population with the following characteristics:

- A culturally and ethnically diverse student body representative of the young Canadian population at large.
- A student body with varying levels of awareness about the risks of online networking – ranging from students in information technology and engineering programs to those in social work, film and arts programs.
- An undergraduate and graduate student body that places an increasing emphasis on preparing for professional life as it nears graduation.

These characteristics of the student body will ensure detailed and representative results with respects to the practices of online social interaction among Canadians in their late teens and early twenties, their perception of privacy and their awareness of the potential risks of online personal information.

The report provides recommendations, based on this insight and on existing organizational practices that inform business and policy makers about best practices, guidelines and policy development to protect personal information online.

Specifically, this report addresses and provides the following objectives:

- Determining the forms of online social networking currently in use by young Canadians.
- Reviewing the nature of risks associated with the use of the Internet for online social networking
- Determining the levels of awareness to various risks associated with the availability of personal information online among young Canadians
- Exploring whether the concept of privacy is understood by online socialisers as protecting dignity or expressing personal control
- Describing the practices and policies of employers about accessing employee or potential employee personal information available online
Methodology

We conducted this project in two phases: Phase 1 centered on the development and administration of a quantitative survey directed toward young Canadians, specifically undergraduate university students; Phase 2 involved a series of in-depth interviews with executives in Canadian organizations.

Phase 1: Quantitative Survey of Young Canadians

Research into the perceptions of risk associated with online social networks (OSNs) began in September 2007. A series of five focus groups provided insight into the ways in which young Canadians use OSNs, their thoughts about privacy and security issues and the language they use to communicate in the online environment.

We used the information gained from these focus groups to develop and refine a quantitative instrument. The resulting 122-item, self-complete questionnaire contained a series of mainly closed-ended questions relating to demographics, attitudes, beliefs and behaviours around online socializing and the perceptions of risk associated with this activity. In addition, we asked respondents to complete two open-ended questions to indicate their primary concern with OSNs, first in relation to their personal life and again in relation to their professional or work life. The questionnaire is attached to this report as Appendix A.

The Sample

A total of 2,300 questionnaires were distributed by hand during the first two weeks of October 2007 to undergraduate students on the campus of Ryerson University – a large, culturally diverse urban Canadian university located in Toronto, Canada, with an enrolment of 23,000. Of these, 294 submissions were eliminated because they were either incomplete or illegible, resulting in a total of 2,006 questionnaires that were used for the final analysis.

As illustrated in Chart 1, students ranged in age from 17 to 39, with over 94% falling into the 18 to 24 category. We used a quota sampling framework to reflect actual enrolment proportions across the entire student body. Charts 2 through 4 confirm the sample represented students enrolled in each year of undergraduate study and across all five Faculties at Ryerson University with almost equal representation of males and females. Furthermore, as shown in Chart 5, the majority of students (70%) work in paid employment on average for at least a few hours per week while going to school.
Chart 1: Respondent Age

Chart 2: Respondent Year of Study
Chart 3: Respondents by Ryerson Faculty

Chart 4: Respondents by Gender
Analytical Approach

We analysed the results of the closed-ended questions from the quantitative survey using SPSS Version 16. Basic summary statistics included frequency distributions and mean values for scale questions.

In addition, cross-tabulations with Pearson chi-square tests for significance, and one-way ANOVA tests were performed to investigate response differences by gender, age, year of study and employment. We chose these variables for the purposes of subgroup analysis as our initial focus group research seemed to indicate attitudinal and behavioural differences between males and females, as well as possible differences among older students who were closer to graduation and therefore likely more concerned than their younger counterparts about their projected online image among potential employers. In addition, students who were already working in part-time positions, particularly those with more than entry-level responsibilities, seemed to show greater awareness of and concern for their reputation. Despite these anecdotal findings, our analysis shows no significant differences by age, year of study or employment in the quantitative study. However, the results of the quantitative analysis do support the focus group research with respect to differences between males and females. These differences are discussed further in the Results section of this report.

Responses to the two open-ended questions were reviewed and grouped according to common themes by a team of three research associates, in consultation with members of the research
team. In order to protect the confidentiality of students, direct quotes presented in this report are attributed by field group number rather than by using personal information.

**Phase 2: Organizations**

We conducted sixteen in-depth interviews with Canadian executives in key decision-making positions to gain their corporation’s perspective on OSNs in January-February 2008. Organizations were approached based on media reports about their use of OSNs, and on information gathered by the research team that indicated the organization had a presence on OSNs. From this larger sample, the research team contacted organizations in federally regulated industries of particular interest to the OPC, as well as organizations from other industries with which the Ted Rogers School of Management has existing contacts, such as the telecommunications, financial services, retail, professional services and hospitality sectors. A total of 49 potential executives were approached and 16 agreed to participate, resulting in a response rate of approximately 33%. Interview participants represent a cross section of six different industry sectors as well as position within the organization, as shown in Table 1:

<table>
<thead>
<tr>
<th>Interview Number</th>
<th>Type of Industry</th>
<th>Type of Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hospitality</td>
<td>Manager</td>
</tr>
<tr>
<td>2</td>
<td>Financial Services</td>
<td>Vice-President</td>
</tr>
<tr>
<td>3</td>
<td>Financial Services</td>
<td>Senior Manager</td>
</tr>
<tr>
<td>4</td>
<td>Retail</td>
<td>President</td>
</tr>
<tr>
<td>5</td>
<td>Professional services</td>
<td>Managing Partner</td>
</tr>
<tr>
<td>6</td>
<td>Financial services</td>
<td>Legal Counsel</td>
</tr>
<tr>
<td>7</td>
<td>Financial Services</td>
<td>Vice-President</td>
</tr>
<tr>
<td>8</td>
<td>Professional Services</td>
<td>Legal Counsel</td>
</tr>
<tr>
<td>9</td>
<td>Hospitality</td>
<td>General Manager</td>
</tr>
<tr>
<td>10</td>
<td>Communications</td>
<td>Manager</td>
</tr>
<tr>
<td>11</td>
<td>Communications</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>12</td>
<td>Communications</td>
<td>Manager</td>
</tr>
<tr>
<td>13</td>
<td>Professional Services</td>
<td>Managing Partner</td>
</tr>
<tr>
<td>14</td>
<td>Public Sector</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>15</td>
<td>Public Sector</td>
<td>Privacy Officer</td>
</tr>
<tr>
<td>16</td>
<td>Retail</td>
<td>Legal Counsel</td>
</tr>
</tbody>
</table>

The interviews were conducted face-to-face in the office of the interviewee by one or two members of the research team and lasted approximately one hour. All interviews were audio-
taped and notes were taken to supplement the tape recordings. We used a semi-structured interview schedule based on the study objectives. The schedule is attached as Appendix B to this report. Some questions required modification, depending on the participants’ area of responsibility within their organization. For example, those working in a Human Resources capacity had different experiences with and perspectives of social networking compared to those working in Marketing.

All interviews were transcribed verbatim, and interviewees were given the opportunity to review either the transcribed interviews or the notes taken during the meeting and to ask for corrections to be made. The final transcripts/notes were reviewed independently by two members of the research team. Subsequent meetings were held to discuss identified themes, issues and trends and to discuss areas where differences in opinion had occurred. Results of the combined analysis are presented in the “Perspective of Organizations” section of the report. In order to protect the confidentiality of participants, direct quotes are attributed by interview number, as shown in Table 1 above.
Results of Quantitative Survey of Young Canadians

The quantitative phase of the project provides critical insights into the use of OSNs by young Canadians and their perceptions of risks and privacy.

Use of the Internet and Online Tools

Chart 6: Usage of Online Tools

Usage patterns of technology tools continue to evolve. As Chart 6 shows, young Canadians report using e-mail, instant messaging and online social networks most frequently. E-mail has the highest usage rate, with 97% logging on to e-mail at least once per week. Instant messaging sites are second in popularity, followed closely by OSN sites (81% and 74% respectively use these at least weekly). Other technologies, such as chat rooms, list servs and bulletin boards are used much less often. Despite much media attention to blogs, they are not currently used much by young Canadians.
As Chart 7 suggests, Facebook is the most popular social network among young Canadians. Ninety eight percent of respondents have heard of it; 92% are members of Facebook; and 89% report it as their most preferred network. As a result, most of the subsequent questions in this section have been answered in the context of Facebook.
As Chart 8 indicates, over 70% of respondents log onto Facebook at least once a day, and for almost half of respondents, there are multiple logins on a daily basis. Such use of Facebook among young Canadians appears similar to the use of e-mail. The level of activity reported specifically for Facebook use appears higher than that reported in Chart 6 for OSN use in general. It appears that the term “online social network” may be somewhat unfamiliar to some respondents, until it is connected with concrete examples such as MySpace or Facebook. The reported usage levels suggest OSNs have become firmly integrated into the communication preferences of young Canadians. As a result, Canadian employers face challenges with respect to managing the use of OSNs among this new generation of employees. As well, opportunities exist to leverage this new capacity to reach large numbers of individuals (employees, customers, general public).
As Chart 9 indicates, young Canadians appear very comfortable posting a large amount of what others might view as personal and private information on their OSN. For example, about 7 out of 10 respondents post their full real name on their home page. In addition, the majority of respondents have posted a portrait of themselves (76%) and/or a group photo that includes their picture (67%). There is also no hesitancy in providing information about their interests or hobbies (61%), favourite music, books, and movies (59%), and even their relationship status (60%). While only a few include traditional contact information (7% provide a full address and 15% list a telephone number), indirect information that could allow others to trace someone’s whereabouts is common. For example, social networks such as Facebook encourage members to identify their home town (74%), high school (69%) or even their employer (31%).
As Chart 10 suggests, there is a relatively low level of concern among young Canadians about people they know accessing information posted on their OSN. Approximately 88% of respondents are unconcerned about having friends access their social network profile and only about 6% express any concern at all with respect to friends' access. This is likely because the intended purpose of the network is to share information among a community of friends. However, there are higher levels of concern with other groups of individuals gaining access to their online information. While slightly more than half of young Canadians remain unconcerned about family members, including parents, seeing their profile, others (about one-quarter) would rather not have family members, particularly parents, gain access. Similarly, while 4 out of 10 respondents don’t mind their employers viewing their online information, another 35% are concerned about this happening. The highest level of concern (almost 45%) relates to worries that people whom the respondent does not know will gain access to personal information. The results presented in Chart 10 strengthens the notion that individuals have the perception of a group- or network-related privacy. They believe that information within this network is private and should not be disseminated outside their selected network.
We asked respondents about the actions they take to protect their privacy and restrict access to their personal information. In terms of awareness of privacy issues, Chart 11 indicates a little over 40% report actually reading the privacy policy provided by their OSN and understanding its terms. Interestingly, approximately 70% report having adjusted the privacy settings on the OSN, thereby actively demonstrating a desire to restrict access to their information. A little over half (54%) of respondents have blocked a specific person from accessing their page and almost 3 out of 10 have experienced someone unknown to them trying to get access to their network. About 13% report having actually contacted the network developers to report distasteful or disturbing content, although most users do not actually view the OSN as primarily responsible for such content, as we will discuss below.

**Online Social Networks at Work**

Since 70% of our respondents indicated that they have a least some work experience, we asked questions related to the use of OSNs in the workplace.
As Chart 12 shows, about 30% of respondents have their immediate supervisor included as a member of their OSN, and nearly 1 in 5 have been approached by a supervisor to be added to their OSN. In addition, 19% of senior executives in the respondent’s workplace are members of their OSN, although only 10% report having a senior executive ask to be put on their OSN. According to respondents, only about 10% of the companies for which they work have encouraged the use of OSNs for business purposes, and approximately 20% have a formal policy related to workplace use.
Within those organizations reported to have a formal workplace policy for the use of OSNs, equal proportions of respondents indicate that use of these networks during company time are forbidden, not forbidden or they don’t know. According to Chart 13, among those who work for a company that prohibits the use of OSNs, few employees appear to abide by the policy (23%), which probably accounts for the practice of some organizations, discussed below, to not only prohibit online socializing, but also to technologically block access to OSNs from work.

Respondents were also given the option to elaborate on their employer’s policy regarding OSNs through an open-ended question. Only a small number (less than 3% of respondents) provide additional information. Those who do, indicate that their employers’ polices range from very restrictive to more lenient. At the restrictive end of the continuum, some employers prohibit computer access for all but management staff, while others allow their employees to use computers, but without Internet access. In a few instances, respondents report the workplace policy includes termination for employees caught using OSNs during work hours. Towards the more lenient end of the spectrum, several people indicate that OSN use is allowed, but only during break times, or with the restriction that clients cannot be added to employees’ OSN lists. In some instances, employees are not permitted to belong to social network groups deemed to be “inappropriate” by the company.
Risk and Responsibility Scenarios
We created four different scenarios related to OSNs involving different types of privacy breaches and asked respondents to report their experience with the scenario, their perception of who was responsible for the negative outcome, and then respond to a series of attitudinal questions related to their use of and beliefs about OSNs in light of the situation described in the scenario. A fifth scenario presented a work-related situation that the respondents might be faced with in the future as managers, and within that context we asked them about the appropriateness of certain actions related to the use of OSNs in the workplace.

The scenarios were developed through focus groups, using elements raised by group participants and elements from media reports. Situations presented in each scenario range from those that were perceived to be realistic or possible by focus group participants to situations that were perceived as less likely. The scenarios provide an indicator of the privacy perceptions of participants, by gauging the reaction of participants to increasingly significant breaches of privacy as the scenarios proceed. The scenarios also gauge whether participants perceive the OSN as having greater responsibility and a greater role to play in the control and restriction of the dissemination of their personal information, as the extent of familiarity decreases between the participant and the individuals accessing and disseminating their personal information.

Scenario 1: Relationship Breakup
In this scenario, a person who is a prominent and trusted member of the individual’s social network is revealed as untrustworthy:

“You have just broken up with your significant other. You are shocked to see that the day after the breakup, your previous significant other posted compromising and what you thought were very private pictures of you on the social network. In addition, this person posted nasty comments that painted a very negative picture of you as a person. As a result, some people whom you thought were your friends have dropped you and you are no longer included in social events.”
As Chart 14 illustrates, while only 3% of respondents have had such an event happen to them, a further 13% know someone personally to whom this is happened. In addition to those who have directly or indirectly experienced a breach of privacy and trust resulting from a relationship breakup, it appears the majority of young Canadians accept this as a likely occurrence, since an additional 45% report they believe it has happened to others.
Chart 15: Responsibility for Adverse Social Consequences

The results presented in Chart 15 suggest that 72% of respondents believe the person who posted the content is most responsible for the consequence of being dropped by friends and no longer being included in social events. Another 42% assign blame to their supposed friends who drop them after the incident. Only about 1 in 4 assume personal responsibility for this incident and less than 20% feel that the network developers should be held accountable.
As Chart 16 indicates, after reflecting on the implications of this scenario, 60% of respondents believe they have taken the appropriate steps to limit access to their personal information. This seems to indicate a sense of control with respect to their ability to manage their OSN information and maintain some level of privacy. However, at the same time a similar proportion (63%) report that if this incident happened to them in the future, they will be much more careful of who is taking pictures of them. Similarly, over 45% are concerned about material posted about them on the network that originates from other sources, and very few (12%) see this as being a harmless prank.
Scenario 2: Party Time

In this scenario, an unwitting lapse in judgment in an offline social setting results in a breach of trust by a friend in the online network, with embarrassing consequences:

“It was your birthday and you went out with friends for a night on the town. You had a wonderful time, drank way too much and really can’t remember most of the evening. The next day you see pictures of your escapades posted on one of your friend’s pages and tagged to you. Your family members see these pictures, are very upset with you and say they can no longer trust you.”

Chart 17: Party Time Scenario: Has this Happened?

Chart 17 suggests that one in four respondents have either had this happen to them or know someone to whom this has happened. Nearly 40% report hearing that it has happened to others and are thus likely to accept this scenario description as one that could plausibly occur.
In terms of who is viewed as responsible for the consequences of these actions, Chart 18 indicates almost two thirds of respondents are prepared to assume responsibility for their actions in this circumstance. However, they are almost as likely to assign blame to the person who posted the content (58%), while very few (10%) feel the network developers should be held accountable.
As Chart 19 demonstrates, family is very important to this age group, in that almost two-thirds report being more upset about their family seeing compromising pictures of them than other people seeing them. In terms of having control over their personal information, 55% feel it is not right when people have access to information not intended for them, and thus the behaviour described in this scenario is certainly not considered a harmless prank. In reflecting about the consequences of such a scenario, more than half of respondents (53%) would be more careful about how they behaved in public in future. Interestingly, despite this concern about family, very few (15%) currently admit to using the social network to keep track of siblings or relatives.
Scenario 3: False Charges

The first two scenarios focus on the level of familiarity and network affiliation between the individual and the person disseminating their personal information. In this scenario, the focus is not on that relationship, but on the possibility of recourse from other sources, and whether individuals view OSNs as shouldering some of the responsibility for such scenarios, or whether they are passive, mere ‘walls’ (to use Facebook’s terminology) on which active users post content:

“Anonymous comments circulate on the online social network about your having been arrested for shoplifting. This is not true and you are shocked to see that these comments have made the rounds to all your friends. No matter what you say, everyone believes you are a shoplifter.”

Chart 20: False Charges Scenario: Has this Happened?

According to Chart 20, while this scenario is less commonly thought of as something that is likely to happen in the online environment, a small proportion of respondents (7%) have experienced a similar situation or know of someone to whom it has happened.
Chart 21: Responsibility for Defamatory Content Consequences

Chart 21 shows that over 80% of respondents believe that the person who posted the content is responsible for the consequences described in this scenario. Their frustration is then projected to the friends who believe the unfounded accusations. Once again, very few (16%) consider the network developers to be responsible for this incident, and even fewer (14%) consider themselves to be at fault.
The attitudes of respondents toward this scenario are depicted in Chart 22. Few believe it is a harmless prank, especially since many feel powerless to do anything themselves to fix it. It is in this scenario more than in any other that respondents feel the developers have a role to stop this kind of erroneous information from being posted. Perhaps this is because being wrongly accused of illegal behaviour has potentially more serious implications than situations in which behaviours are viewed as “social mishaps”. However, rather than relying on the network developers to correct the problem, a substantial proportion (44%) feel the developers should release the name of the person who posted the lie, so that they can take their own action. Fewer respondents in this scenario than in others feel they are able to take appropriate steps to control what is posted about them on their OSN (38% versus 60% in Scenario 1).
Scenario 4: Sick Leave

In this scenario, focus is on the workplace implications of online personal information disclosed outside of the social network:

“You called in sick to work, because you really wanted to go to your friend’s all day graduation party. The next day you see several pictures of you having a great time at the party. Because the pictures are dated, you start to worry about whether you might be caught in your lie about being sick. You contact the developers of the social network and ask that the pictures be taken down because the tagging goes so far, it would take you too long to find all the pictures. There was no response from the network. You are stunned to be called in by your supervisor a week later to be advised that you were being “written up” for taking advantage of sick leave and put on notice that if it happened again you would be terminated.”

Chart 23: Sick Leave Scenario: Has this Happened?
According to Chart 23, 15% of respondents have been involved in a similar incident themselves or know someone personally to whom this has happened. Another 30% report having heard of it happening to others and therefore would be inclined to accept the incident as plausible.

**Chart 24: Responsibility for Adverse Workplace Consequences**

The data in Chart 24 suggest that over three quarters of respondents believe they are the ones responsible for the consequences of their behaviour in this instance. A further 37% believe the person who posted the material on the OSN is also responsible. Remarkably, despite attempts to contact the network developer and receiving no response, only 11% of respondents hold the developer accountable for this incident.
According to Chart 25, about half of the respondents again express concern about material posted online that does not originate with them and believe others should not have access to information not intended for them. While 4 out of 10 respondents believe the developers should have responded immediately to the request to have the material removed, only a few (13%) hold the developers legally liable for the consequences that ensue, even if those consequences include termination from their workplace. As with the previous scenarios, most respondents do not view this situation as a harmless prank.

**Scenario 5: Workplace Uses of Online Social Networks**

The final scenario asks individuals to role-play, and envision themselves as recipients of the personal information of others, rather than as the individual affected by the disclosure of their own information:

“In this scenario, assume that you are a manager with five employees. You are in your early thirties and your employees are in their twenties. How appropriate is it for you to; (a) Use a social network to check up on what your employees do during their personal
time without them knowing; (b) Require your employees to add you as a ‘friend’ to their social network; (c) Use a social network to check out the character of someone who has applied for a job; (d) Proactively research social networks to identify potential high quality candidates for future positions.”

Chart 26: Employer Use of OSNs

As Chart 26 demonstrates, respondents feel it is somewhat or very inappropriate to use social networks to check up on employees (77%), to require employees to add you as a “friend” (80%), to use a social network to check out the character of someone who has applied for a job (60%) or to research social networks to identify high quality candidates for future positions (50%). They feel less strongly about the inappropriateness of using the OSN for after hours purposes when socializing with their employees (28%) or when promoting goods and services through the network to users (35%).
Respondents were asked for their views about the role of OSNs in the workplace. As Chart 27 illustrates, more than half (56%) of respondents maintain that work life should be kept separate from personal life and what they do in one should not affect the other. As a result, 49% support the blocking of OSNs at work. These individuals clearly anticipate that their use of OSNs will change as they more fully enter the workforce. However, a similar proportion (52%) disagree that someone with career ambitions should avoid membership in OSNs, or that knowing how a person behaves outside of work hours gives managers insights into whether a person is promotable (56% disagree). In terms of marketing, more respondents see the potential of OSNs as a tool for promoting good and services (56%) than do those who see it as a mechanism for learning more about customers (32%).
Comparison of Responsibility Assignment across Scenarios

Chart 28: Perspectives of Responsibility

Each scenario presents a different situation with respect to roles, responsibilities and consequences. Interestingly, as summarized in Chart 28, regardless of scenario, respondents appear to point the finger of responsibility either at themselves or the person posting the content. They tend to be less inclined to find fault with those involved in meting out the consequences and seem to have particularly low expectations of the network developers.

Sub-group Comparisons: Gender and Year of Study

We examined responses to the five scenarios by age, year of study, employment and by gender. Our focus group research seemed to indicate that the closer students were to entering the workforce full-time, the more concerned they were about their reputation and the risks of activities on OSNs, and the more aware they were of the permanent nature of their OSN “trail” and the difficulty of “scrubbing” their electronic record clean. Similarly, those currently employed, even on a part-time basis, seemed to show greater awareness of the potential risks
of inappropriate OSN activities from their employer’s perspective. Despite these anecdotal findings, there were no significant differences by age, by year of study or by employment status in our quantitative survey. Our focus group research also suggested that there would be differences between males and females in how they assessed and reacted to threats to their online privacy and security. The quantitative results support the focus group research with respect to differences between males and females. The findings are reported in detail in the following sections.

**Scenario 1: Relationship Breakup**

With respect to Scenario 1, males are significantly more likely than females to report having had something similar happen to them or to someone they know (20% vs. 14%).

In terms of who is responsible for being dropped by the people who were previously thought to be friends and being excluded from social events, Chart 29 presents the mean values on a scale of 1 to 5 where 1 does not reflect my views at all and 5 reflects my views very well.

**Chart 29: Responsibility for Adverse Social Consequences by Gender**
Both males and females believe that the person who posted the material is responsible for the negative consequences, but females are significantly more likely to assign blame to this person (p=.000). Respondents also feel that friends have some responsibility for this outcome, and once again females are significantly more likely than males to hold this belief (p=.001). Overall, respondents do not see themselves or the network developers as having responsibility in the outcome. However, males are significantly less likely than females to believe that developers have a role (p=.004).

Respondents were also asked to report their views on a series of privacy issues raised in Scenario 1. The mean values are reported in Chart 30 (using a scale of 1 to 5 where 1 does not reflect my views at all and 5 reflects my views very well).

**Chart 30: Reactions to Posting of Damaging Material by Gender**

![Chart 30: Reactions to Posting of Damaging Material by Gender](chart30.png)

---

14 A "p" value refers to the probability that the differences observed between two or more groups (the independent variables) in response to an issue (the dependent variable) are the result of a real difference between the groups and not because of chance. For a statistically significant result p must be smaller than .05, which means that 95 out of a 100 times the observed differences in response on the dependent variable are because of the group differences (the categories of the independent variable) and not because of chance. References to p=.000 indicate a less than 1 chance in 1000.
Both males and females believe that they take the appropriate steps to limit who has access to their profile, but females have a significantly stronger belief (p=.000). Perhaps because of the belief that they have done what was needed to protect their privacy, both males and females report that they will adjust their behaviour if this scenario happened to them. However, females are significantly more likely than males to indicate they will be much more careful about who is taking their picture (p=.000), and significantly more likely to say they will be more careful in how they treat other people (p=.000). Similarly, respondents are concerned about material that is posted on the network that does not originate with them, but females are significantly more concerned (p=.000). Finally, respondents do not view the consequences of this situation as being a harmless prank, females significantly less so than males (p=.000).

Scenario 2: Party Time

In Scenario 2, although males are slightly more likely than females to have had something similar happen to them or to someone they know, the differences are not statistically significant (26% vs. 23%).
In terms of who is believed to be responsible for the family’s being upset and no longer trusting the person involved in this scenario, Chart 31 presents the results.

Both males and females believe that they will be responsible for the negative consequences of this situation, with females holding this belief significantly more than males (p=.009). In addition, the person who posted the content is also viewed as responsible, and once again females hold this belief more strongly than males (p=.000). While neither males nor females see family members or developers of the network as being responsible for these negative consequences, females are significantly less likely than males to assign blame to family members (p=.018).

Respondents were also asked to report their views on a series of privacy issues raised in Scenario 2. These findings are reported in Chart 32.

**Chart 32: Reactions to Posting of Embarrassing Material by Gender**

While both males and females report being more upset with family seeing pictures versus acquaintances, females report being significantly more upset than males (p=.000). If respondents had this happen to them, they indicate they will be more careful about how they
behave in public, females significantly more so than males (p=.000). Females are also significantly more likely to report concern about people having access to their private information (p=.000). Neither males nor females use an OSN for keeping track of the behaviour of siblings or relatives. Not surprisingly, neither males nor females view this situation and its consequences as a harmless prank. Females are significantly more likely to hold this opinion (p=.003).

**Scenario 3: False Charges**

This situation shares some of the characteristics of the two previous scenarios in that unwanted information is shared over an OSN. What differentiates this situation from others is that the posted material is not true, and the consequences may have legal implications. In terms of who is believed to be responsible for the circulation and consequences of this erroneous information, Chart 33 presents the results.

**Chart 33: Responsibility for Defamatory Content Consequences by Gender**

Respondents are clear that they would not view themselves as responsible in this type of situation, and equally clear that the person who posted this material bears most of the
Respondents were also asked to report their views on a series of privacy issues raised in Scenario 3. The findings are reported in Chart 34.

**Chart 34: Reactions to Posting of Defamatory Material by Gender**

![Chart 34: Reactions to Posting of Defamatory Material by Gender](image)

Neither males nor females believe that they should be able to count on the network developers to stop this. On the other hand, they do believe that the developers of the social network should tell them the name of the person posting the erroneous information. Respondents continue to believe that they have set up the appropriate privacy controls, and thus situations like this make them feel helpless about protecting themselves. Females are significantly more likely to report feeling helpless (p=.000). Given these beliefs, it is also not surprising that respondents do not view this situation as a harmless prank. Again, females are significantly more likely than males to hold this belief (p=.007).

**Scenario 4: Sick Leave**
The important feature of this scenario is that the situation involved career consequences. Males are significantly more likely than females to have had something similar happen to them or to someone they know (18% vs. 13%). In terms of who is believed to be responsible for these potential career consequences, Chart 35 presents the results.

**Chart 35: Responsibility for Adverse Workplace Consequences by Gender**

Respondents believe that they are primarily responsible for this situation, with females holding this belief significantly more than males (p=.000). They do not see the person who posted the content or the developers has being responsible, which is somewhat surprising given that the developers were asked to remove the content. Likewise respondents do not see the supervisor as responsible, particularly female respondents (p=.020).

Respondents were also asked to report their views on a series of privacy issues related to Scenario 4. The mean values are reported in Chart 36.
Respondents express concern about access to their private information by people for whom it was not intended, and that material posted about them on the network does not always originate with them. For both items, females feel significantly stronger about this access than do males (p=.000 and p=.000). Similarly, females are significantly more likely than males to view this as not just a harmless prank (p=.006). Respondents do not feel that the developers of the network can be legally liable if a termination occurred, although they marginally feel that the developers should have responded immediately to the request to remove the material.

Scenario 5: Workplace Uses of OSNs

Respondents were asked to evaluate the appropriateness of various actions listed in Chart 37 on a scale of 1 to 5 where 1 is not very appropriate and 5 is very appropriate.
Respondents, especially females feel very strongly that it is inappropriate for managers to either use a social network to check up on employees (p=.009) or to require employees to add them to their friends’ list (p=.010). Likewise respondents, especially females, do not feel it is appropriate for managers to use a social network to check out a job applicant (p=.000), or to search for potential applicants (p=.000). Males are significantly more likely than females to feel that it is acceptable for managers to socialize with employees on an online network (p=.000) and to use the network as a marketing vehicle for company goods and services (p=.018).

We also asked respondents to agree or disagree with statements about various uses of OSNs using a scale of 1 to 5 where 1 is strongly disagree and 5 is strongly agree, as reported in Chart 38.
Both males and females believe that OSNs should not be accessed during work hours and females are significantly more likely to hold this belief \((p=.004)\). Respondents believe that work life should be separate from personal life and that OSN behaviour does not provide insight into suitability for promotion. Neither males nor females see career threats related to participation in OSNs, and males are significantly more likely to hold that view \((p=.031)\). Respondents, especially males \((p=.022)\) are even stronger in their views in this set of questions that online networks have marketing potential. In contrast, respondents, especially females \((p=.000)\) are less likely to see OSNs as a viable mechanism for learning more about a company’s customers.

**Gender Differences Summary**

As could have been expected young women are more aware and more concerned about their privacy and their reputation. Young women are therefore more active in their attempts to control access to their personal information and through it to control their reputation. Young men are more likely to discount and dismiss OSN-related risks, and therefore more open to the possibility of other uses of OSNs beyond their primary social function. Young women have a greater expectation of network privacy than do young men.
Open-ended Comments

Personal Life Concerns
At the end of the survey questionnaire, young Canadians were asked to complete two open-ended statements. The first statement was: “With respect to my personal life, the thing that worries me most about being on an online social network is…” Table 2 presents the categorization of responses by frequency.

<table>
<thead>
<tr>
<th>Table 2: Frequency of Issues Identified Related to Personal Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. General privacy concerns – 171</td>
</tr>
<tr>
<td>2. No Explicit Access Given – Stranger Concerns</td>
</tr>
<tr>
<td>a. Random/Strange Access Concerns – 265</td>
</tr>
<tr>
<td>b. Physical Safety (Sexual Predators) - 11</td>
</tr>
<tr>
<td>c. Economic/Fraud – 69</td>
</tr>
<tr>
<td>d. Emotional Safety - 253</td>
</tr>
<tr>
<td>▪ People actively and repeatedly collecting info (i.e., stalkers) – 151</td>
</tr>
<tr>
<td>▪ People actively collecting info (i.e., creepers) - 43</td>
</tr>
<tr>
<td>▪ People with ill intentions / pose a threat – 59</td>
</tr>
<tr>
<td>e. Business - 16</td>
</tr>
<tr>
<td>3. Given Access – Relationship Concerns</td>
</tr>
<tr>
<td>a. Reputation/Image – 373</td>
</tr>
<tr>
<td>b. Family/Parents – 91</td>
</tr>
<tr>
<td>c. Romantic Relationships – 28</td>
</tr>
<tr>
<td>d. Employment Concerns – 21</td>
</tr>
<tr>
<td>e. Social – 36</td>
</tr>
<tr>
<td>4. Wasting time/Addiction – 27</td>
</tr>
<tr>
<td>5. Other – 51</td>
</tr>
<tr>
<td>6. No Concerns– 202</td>
</tr>
<tr>
<td>7. N/A or No Response – 81</td>
</tr>
<tr>
<td>Total – 1652 Responses</td>
</tr>
</tbody>
</table>

As the frequency distribution suggests, two distinct concerns emerge. The first is about situations in which no explicit access to personal information had been given; and the second involves concerns about access to information by those with whom the respondent already has
an established relationship. Other concerns are more general in nature and are expressed simply with phrases related to “privacy” or “personal information”, “distraction” and “wasting time”. About 17% of respondents indicate they have “no concerns”. Chart 39 to 41 present a graphic representation of these concerns.

**Chart 39: OSN Concerns Related to Personal Life**
1. General Privacy

In this category, respondents express concerns about general privacy and participating in OSNs. They express worries about “privacy,” “confidentiality” and “security.” The majority of respondents simply write “privacy.” What we know from our quantitative survey and pre-study focus groups is that respondents have different conceptualizations of what these terms actually
mean, but all agree that it has to do with personal space or personal information being shared or broadcast in a way that was never intended by the respondent.

2. No Explicit Access Given – Stranger Concerns
These are concerns expressed about people whom the respondent does not know. These comments are consistent with the quantitative results that show 45% of respondents have at least some concern about strangers accessing their personal profile information. As result, 70% report in the quantitative survey that they have adjusted their privacy settings, which demonstrates their desire to block information. In order for access to the profile to occur on Facebook, the respondent’s privacy settings must be set to allow users to view a profile without direct approval. In other words, either respondents are not aware that they can control access, or they are aware and have not done it, or they are aware and think they have adjusted the privacy settings, but they have not done it correctly. Regardless, it is clear that more information needs to be provided to those using OSNs, so that they understand the control they have over access to their information, and they know how to adjust the settings to limit access.

Responses that are more specific were subdivided into more descriptive categories including physical safety, economic security, emotional security and concerns with business used.

a) General Concerns with Random People (265 responses, 16%)
These concerns relate to people whom the respondent does not know and whom the respondent believes have not been given explicit access (i.e. strangers, random people). In this general category, there is no elaboration of the concern (i.e. safety concern). Examples of the responses in this category include:

- “People I don’t know having access to info” (g72)
- “Not being able to control who sees my profile” (g40)
- “That my pictures can be easily spread and access by people I don’t know” (g43)
- “What strangers can find out about you” (g15)

b) Physical Safety Concerns (11 responses, 1%)
These are concerns specifically regarding predators (i.e. online, sexual).

- “Sexual predators using information to attack me” (g21)
- “Pedophiles trying to get to younger children who have an online social network” (g74)

c) Economic Security Concerns (69 responses, 4%)
These are concerns relating to economic security, including: identity theft, fraud, robbery, scams, and hackers.

15 The designation refers to the fieldwork group that collected the data from this respondent. Each fieldwork group was assigned to collect data from 50 to 100 students within a specific program/school/department within the university.
PRIVACY AND CYBER CRIME INSTITUTE

- “People using my information to apply for credit cards etc” (g6)
- “People using my name” (g77)
- “Identity theft” (g16)
- “People hacking / having access to computer/ personal files” (g22)

d) Emotional Security Concerns (253 responses, 15%)
These are concerns with emotional security, where “unknown” people were identified as threatening in some sense. This category has been subdivided according to the “type” of threat:

i) People actively and repeatedly collecting info (151 responses, 9%) - i.e. Stalkers
   - “Being stalked by strangers” (g46)
   - “People checking up on me and people stalking me” (g9)

ii) People actively collecting information (43 responses, 3%) i.e. creepers, lurkers, spying
   - “People creeping on my profile” (g24)
   - “Being monitored by someone I don’t know” (g37)
   - “People can track everything about me” (g42)

iii) People with ill intentions or those who could pose a threat (59 responses, 4%) i.e. wrong people, bad people, weird people, crazy people
   - “Being found by potentially dangerous people” (g30)
   - “My personal information getting into the wrong hands” (g19)
   - “People knowing where I live” (g18)

There are two interesting observations about this set of comments. First, a language is developing around this unauthorized access: stalkers, lurkers, creepers. Second, some of this language is borrowed from another context (e.g. Stalker, a “creep”), but it is applied in this context differently. Stalking in the traditional sense of the word is much more physically threatening, and calling someone a creep is usually as a result of some face-to-face interaction.

e) Concerns with Business Use (16 responses, 1%)
These include specific concerns that personal information is being used by companies for marketing or other business purposes.

- “My personal information being available for companies to send spam mail” (g83)
- “What developers are doing with my personal/private info” (g4)

3. Given Access – Relationship Concerns
For this group of responses, it appears that respondents have given access to their profile, but have concerns about how those seeing the information will view them. This category includes issues related to control over information within their social group where personal relationships already exist. Sub-sets of responses include concerns about romantic relationships, social situations, reputation and image, family or parental relationships, and employment situations. While reputation and image are primary concerns, some responses specify the source of the information as part of the issue; that is whether the content originates from the respondent or others.
a) Reputation/ Image (373 responses, 23%)  
Many respondents express concern about judgments being made about their character and interpretations of their personality based on posted information, as well as the inappropriate use of information. Respondents worry about the “negative” or “wrong” impressions or ideas that may be inferred from the content contained in their profiles or “negative,” “misrepresentative,” “false” or “untrue” statements being made or posted about them by others. This includes concerns about “gossip” and “rumours.” Some also worry about their lack of control about the posting of particular types of personal information (i.e. “compromising” or “unflattering” pictures, negative wall posts) that others may be posting. Several express concern about the excessive amount of information available on the network or report a feeling that “too much” information is now available on OSNs. Specific comments related to these concerns include:
  
- “Having people judge me based on an online profile” (g74)
- “Having very personal information posted about me without any control over deleting/removing it” (g78)
- “I can’t control what others post about me” (g74)
- “Having wrong things said about me. People getting the wrong ideas when viewing my profile” (g32)
- “People judging my character without actually meeting me” (g10)

b) Family/Parent Concerns (91 responses, 6%)  
These respondents are worried about their families or parents viewing or accessing their profile. Pictures, social activities, wall posts and messages being viewed by family members are specifically cited. Part of this concern has to do with the age and stage of the lifecycle of the respondents. Most of them are no longer minors (they are older than 18), but many still live at home and depend on their parents financially. Expectations around behaviour are often tied to that kind of support, at the same time as these young adults are trying to be more independent. These comments are a reflection of that tension.
  
- “My family finding out about my weekend activities” (g90)
- “My family using information/finding out information I did not want them to see” (g40)
- “People seeing inappropriate pictures that are tagged of me by others...like certain family members” (g93)
- “My family seeing pictures they may take the wrong way” (g14)

c) Romantic Relationships (28 responses, 2%)  
Respondents report worries about information being shared online that can affect personal or romantic relationships. Pictures, wall postings and messages that may have been shared inadvertently are mentioned as being misinterpreted by significant others.
  
- “Unnecessary rumours reaching my other half and raising troublesome issues” (g37)
- “That my boyfriend will see something I don’t want him to” (g70)
• “Finding out information that is private from friends or boyfriend from the network first” (g91)

d) Employment Concerns (21 responses, 1%)
Interestingly, these are work-related concerns raised in response to the statement about personal life. Respondents express worries about the blur between personal and work life, about the impact of their profile on their work reputation, and job security.
e) Social Situations (36 responses, 2%)
Some respondents are concerned about the social implications of information available on OSNs. This includes situations in which respondents feel forced into undesirable social interactions, and decreased use of traditional social interaction.
  • “Getting too involved with online friendships instead of real ones” (g31)
  • “People from the past I don’t want to see contacting me” (g66)
  • “Acquaintances seeing pictures/postings that were intended for close friends” (g31)
  • “Having people from different social settings see parts of my life that they are not part of” (g77)

4. Wasting time/Addiction (27 responses, 2%)
Respondents worry that their use of OSNs will be a distraction and take away time or attention from school. This includes “wasting time,” “slacking,” or “procrastinating.” This also includes more serious concerns about becoming obsessed or addicted to OSNs. Given our previous findings, which indicated almost half of our respondents log into their OSN more than once a day, this concern may be quite appropriate.

5. Other (51 responses, 3%)
Responses in this category are vague, the language or writing is difficult to decipher, or the answers are unrelated to the issue under consideration, perhaps because the question has been misunderstood.

6. No Concerns (202 responses, 12%)
Responses in this category explicitly express “no concerns” and are different from the more passive “no response” in that respondents wrote “none” or “no concerns” as opposed to leaving it blank.

7. N/A or No Response (81 responses, 5%)
All responses in this category are either blank or state “N/A.”
Work Life Concerns

For the second open-ended question, respondents were asked to complete the statement: “With respect to my work life the thing that worries me most about being on an online social network is...”

As Table 3 and Chart 42 illustrate, respondents identify a range of worries, concerns and issues related to access to OSNs at work, the damage to reputation that can occur as a result of what is posted, the amount of privacy protection built into online networks, job security and career advancement.

<table>
<thead>
<tr>
<th>Table 3: Frequency of Issues Identified Related to Work Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. General ‘Privacy’ Concerns- 68</td>
</tr>
<tr>
<td>2. Job Security – 107</td>
</tr>
<tr>
<td>3. Personal Life exposure at Work (Access) – 367</td>
</tr>
<tr>
<td>4. Reputation – 433</td>
</tr>
<tr>
<td>5. Intent – 87</td>
</tr>
<tr>
<td>6. Distraction – 24</td>
</tr>
<tr>
<td>7. Other – 54</td>
</tr>
<tr>
<td>8. No Concerns – 364</td>
</tr>
<tr>
<td>9. N/A or Blank – 210</td>
</tr>
</tbody>
</table>

Total – 1627 responses
1. **General Privacy (68 responses, 4%)**

In this category, respondents express concerns about privacy in general. They list worries about “privacy,” “confidentiality” and “security.” Most respondents simply write “privacy,” with no clarifying details about what that means to them.

- “How much privacy I have” (g37)
- “Lack of education by developers of “Privacy Settings.” Lack of “Privacy Options” on the network” (g11)
- “Invasion of privacy” (g47)

2. **Job Security (107 responses, 6%)**

Respondents in this category outline concerns about job opportunities or career status. For example, they worry about being fired or passed over for promotion because of information posted on their OSN profile. Some express a fear that potential employers may be viewing this information or that what is posted on their profile may influence the decision to hire them.

From our in-depth interviews with employers (in the next section of the report), some of these fears may be well founded because employers are considering OSN profiles as an additional source of information, although few have currently developed formal plans to include this in their selection strategies. Employers also tell us that if employees post material deemed to be
confidential or unflattering to the company that disciplinary action is guaranteed in the former and possible in the latter. Respondents comment on job security issues as follows:

- “Whether or not an employer will make a decision on hiring me or not based on my profile” (g68)
- “Not getting jobs because I come across as irresponsible” (g35)
- “Being fired for stuff that is posted on the Internet” (g21)
- “Whether my personal life will appear negatively in the consideration for my advancement professionally” (g13)

3. **Personal Life Exposure at Work - Access (367 responses, 22%)**

These respondents express concern about employers or co-workers gaining general access to their OSN profiles. They worry about their personal life (through the information, pictures, comments on their profile) crossing over to their work life, if workmates view their profiles. This category also includes general concerns about the blurring of personal and work life. As our in-depth interviews show this to be an issue with which employers are struggling, these concerns appear well founded.

- “Employers seeing my profile and pictures” (g92)
- “My boss finding out about my weekend activities” (g90)
- “My employer seeing me and my personal life” (g41)
- “That my personal life and my job are not kept separate. I feel like they need to be” (g57)
- “I would like to keep my work and personal life separate and online social networks can often make this difficult” (g95)

4. **Reputation (433 responses, 26%)**

These responses specifically relate to image or reputation within the workplace. Consistent among them is a concern about coworkers or superiors passing judgment, and being passed over for promotion based on the basis of information available on their profile. Concerns are expressed about judgments being made about both personal character and work ethic.

- “Reputation at work based on social profile” (g46)
- “Employer judging your work skills based on the pictures and information from network” (g46)
- “Having my employer see my profile and him/her doubting me because of things happening in my personal life” (g87)
- “A manager seeing immature acts and believing that it would follow me into the workplace” (g1)
- “Having an employer lose respect for me” (g89)
5. Intent (87 responses, 5%)
These respondents express concern not only about access to personal information by employers and coworkers to their profiles, but also about their workmates actively seeking out information about them. This category includes worries about bosses and workmates “spying,” “checking” or “researching” their personal information.
  • “My boss spying on me” (g86)
  • “My employer keeping tabs on me all the time” (g78)
  • “Managers will stalk me” (g77)
  • “That an employer might look at my profile to check information on me” (g90)
  • “How my co-workers and managers can use my social network to check what I do with my personal life” (g44)

6. Distraction (24 responses, 1%)
Those reporting this as an issue worry that their use of OSNs will be distracting and take away time or attention from work or school. This includes “wasting time,” “slacking,” or “procrastinating.” This also includes respondents who express concerns about becoming obsessed or addicted to OSNs, and having to endure the consequences.
  • “That I might lose focus in my career, job, etc...” (g60)
  • “The temptation of going on and not getting my work done” (g46)
  • “Not getting work done because I am being distracted” (g67)

7. Other (54 responses, 3%)
Responses in this category are vague, the language or writing is difficult to decipher, or the answers are unrelated to the issue under consideration, perhaps because the question has been misunderstood.
  • “Where I work” (g13)
  • “Taking bad about my co-workers and managers” (g59)
  • “To contact with business partners” (g63)
  • “My co-workers have more of a social life than me! Ouch!” (g13)
  • “People who add me as a friend and I have not talked to them in over 5 years” (g28)

8. No Concerns (364 responses, 22%)
Responses in this category explicitly express no concerns.

9. N/A or Blank (210 responses, 13%)
All responses in this category are either blank or state “N/A.”
The Perspective of Organizations

The results of the sixteen in-depth interviews conducted with those responsible for privacy in companies and organizations including the public sector, professional services, financial services, retail and hospitality sectors. In order to maintain confidentiality and to protect the privacy of the respondents, comments attributed to respondents are identified by number only, based on Table 1 in the Methodology section of the report.

Awareness and Personal Use of Online Social Networks

Respondents were asked about their awareness of various online networks, how they heard about them, if they use them, and their perspective on their utility from a work perspective. All respondents have heard of Facebook, and about half have heard of LinkedIn. Friends, family and work colleagues are identified as the information sources for these OSNs. Several respondents indicate that they have co-workers and friends on Facebook and have been asked numerous times to join as “friends”. About half of respondents have at least signed onto Facebook and use it at least occasionally to keep track of old friends. One of the most technically savvy respondents has “linked my Facebook profile page to my blog” (8).

Those who use Facebook report using is for social reasons and none of the respondents sees it as a business tool. Age appears to play a role in the comfort level with Facebook with respondents in their 30s expressing fewer concerns with OSNs than do respondents in their 50s and 60s. Even those who use it, pay attention to what is actually posted. “I limit information I put on my public profile to only information I feel comfortable sharing” (1).

Non-users, on the other hand, express their deep concern about the implications and impact of such information sharing. “In terms of putting information on there, I would never in a million years put information about myself or my family on any type of public Internet site”(2) Others express similar sentiments. “Personally, I am horrified that people will have to stoop to this. I can see how it works, but to me, it’s the same thing as hiring a billboard on the 404 some place...I am surprised that more people are not concerned about the consequences of this” (4). Respondents also express concern about the age and naiveté of some users. “The first thing that frightens me terribly is the fact that people who are using it are uneducated as to what happens to the information, particularly the younger crowd....I think for mid-to-late 20s, early 30s, it may be a great social network thing” (4).

From these initial comments, we see that there is much discomfort among business executives about OSNs because of the overriding concern about the long-term and currently undefined consequences of sharing information online. In addition, it is evident that there is a
generational divide about the use of and comfort with this form of communication with the younger generation being more likely to be a member of an OSN.

**Corporate Policies and Practices**

Respondents were asked to describe the policies, if any that exist in their organization to govern the use of OSNs, such as Facebook. All respondents report having either “a blanket policy for Internet usage” (1) also described as “a technology use policy that restricts and directs employee use of e-mail and the Internet for personal use” (5) and/or “a code of business conduct that is intended to regulate our employees’ behaviour” (2) that may “prohibit employees from using the company name, logo or trademarked information” (1) for purposes not related to the company. None of our respondents has a policy specifically focused on the use of OSNs, as there is an implicit assumption that “existing policies on the use of the Web handle this” (4). Likewise, the companies of most respondents block access from work computers to inappropriate sites, such as pornography or gambling.

With respect to OSNs, a number of companies have blocked Facebook and online chat (e.g. MSN) because of concern about productivity and “the burden on the network [because of] the extent of network traffic” (14). As one respondent put it: “I am very conservative...blocks on everything. I tend to think that the best way to approach this is to handcuff everybody’s hands” (6).

However, there have been second thoughts about blocking OSNs among some respondents’ companies because on reflection “it cuts off legitimate networking that was ongoing with the community” (14), and because it represents a “contradictory position” in that the same company that sees it as a distraction for some business units, may be using it as a marketing or recruitment tool in other business units.

Others view the blocking of Facebook as a “knee jerk” (14) reaction, and that a more strategic response would be to try to understand “why is it they go, what motivates them to use it and see to what extent we can use that more generally to enhance our work environment, both the productivity, but even the work/life balance and motivation of employees, and let’s understand where the behaviour is not something that we would want” (14).

None of the organizations has a disciplinary policy regarding the use or overuse of OSNs during work hours, nor do the companies have formal policies regarding the posting or viewing of inappropriate material explicitly on OSNs during work hours. Instead these actions are viewed as covered under the existing policies. For example, “if an employee were to “put information out in the public domain that is confidential about [the company’s] business or that actually is harmful to someone’s reputation, it is a breach of the code of business conduct and will be
dealt with by the appropriate disciplinary action up to and including termination, and in the most extreme cases, prosecution” (2). Further, in terms of OSN postings, “anything that identifies them...as an employee, we would consider inappropriate behaviour and impacting our workplace in a negative fashion, and we would certainly hold that individual accountable” (10).

None of the companies reports any specific terminations that have occurred as a result of the inappropriate use of OSNs, in large part because there is the belief that one “could never really enforce it [a policy]” (14). For example, one cannot “police what people do on their own [personal] computers” (11). However, some companies have tried to extend their code of conduct beyond 9 to 5, so that employees at no time, “are authorized to put up information about [the company] and if we find out you are doing that and if it’s information that causes us concern as it risks the reputation or confidential information, there will be consequences” (2).

In addition, companies respond on a complaints basis to individual incidents. For example, one company “had complaints from employees and from customers about people who were using external OSNs for defamation of a client or to share or disclose information about clients” (11) and the employees were disciplined under the existing code of conduct.

In another instance, a person who had been a satisfactory employee was identified by a customer as moonlighting as a porn star. Although “it was on his own time, but bottom line he worked at a [company location] so customers knew him by walking in and dealing with him. We weren’t comfortable with that, as an association for us as an organization, so we decided to part company” (3).

OSNs are not all negative as pointed out by our respondents. Several have their own internal communication systems for collaborating and sharing ideas and problems. Many are more comfortable with having something internal because they have control over who has access and can shut down inappropriate conversations.

None of our respondents has created a specific corporate policy to govern the use and abuse of OSNs. Instead they rely on existing technology use policies and codes of conduct to deal with any inappropriate behaviour. In addition, they do not look for problems, but instead they wait for them to be brought to their attention. However, when there are issues, they take disciplinary action immediately using the processes outlined in the existing policies. Companies are still working out the norms surrounding the use of OSNs and what is appropriate and not appropriate as they deal with more and more issues involving the use of an OSN as a medium of communication. While the rules with respect to the use of the Internet are fairly clearly defined in our respondent companies, the policy direction with respect to OSNs is still quite murky. OSNs are different enough that simply blocking access may not be the best strategy, and
because companies find it both difficult and somewhat distasteful to be policing what employees do on their home computers and on their own time, codes of behaviour around the use of OSNs and the workplace will continue to evolve.

**Issues and Concerns about Online Social Networks**

Respondents were asked to give their perspective on issues and concerns related to OSNs.

The first issue identified is one of control around the use of the “brand”, and “brand management”, to the extent that a few companies admit to “trademark trolling” (11), that is looking for inappropriate uses of their logos or trademarks by unauthorized persons on the Internet. Several companies encourage employees “not to post any potentially harmful photos on their Facebook page and when possible to not list the company name” (1), because of the potential negative influence of the personal life of an employee on the company’s image. There is also a concern about “employees posting confidential or derogatory information that would pose a risk to the brand and the good name and reputation of the company” (2).

A further perspective on this issue of control is what happens when inappropriate information is posted. “Once the content is out there in the public domain, on the Internet, it is extremely difficult to have it removed” (2). “You have to develop the skills to be prepared to detoxify a neutron bomb that went off while you were asleep because there is no way of being able to control what somebody is going to do or more specifically say in any kind of forum” (4). These respondents, unlike our younger survey participants, do not distinguish between information posted on an OSN where access can be limited and information posted on the Internet where access may be entirely open (e.g., on a web page or blog).

Some respondents see this issue of control as “an education issue” (7). It is important to educate employees on what is an appropriate use or an inappropriate use in the work context of these technologies” (14). However, “setting clear rules in advance is hard....You’ve got to create a policy that sets some broad guidelines, but there is no way you can create a crystal clear rule” (8). So the real challenge is walking the fine line between discouraging inappropriate behaviour, but encouraging appropriate use because “this sort of technology does have potential benefit for business. So we need to be reasonably open to its use for that purpose while still being aware of what the risks are and having a good approach to having a response to those risks” (2). Once again, we see the struggle of companies to identify what should be included in a code of conduct around the use OSN. Although it is a digital medium, it appears to have very different opportunities and threats associated with it than do traditional Internet sites. While several companies recognize that they have no formal control over OSNs and that is a cause for concern, some also have no desire to exert too much control because there is
potential to be leveraged. The dilemma at the moment, is that companies do not understand and cannot articulate what that potential is or could be.

**Work Life / Personal Life Boundaries**

We asked respondents their view on the line between personal and work life and the impact of OSNs on this boundary. There is general agreement that “there is a fine line between the two” (1).

Respondents are also in general agreement that there is a generational aspect in that younger people “have a different view about personal versus private life” (8); and that using Facebook “is part of the youth culture” (5). For the under 30 group, “there is an underlying expectation...that what happens on Facebook stays on Facebook. People aren’t posting things on there and expecting you to run back to their manager” (12). Likewise, “people do things away from work that doesn’t reflect on their personality at work, so if they create something with the expectation that it’s not going to be viewed in the work context, then I think it’s difficult to put them in a place where we are going to say, now we are going to review it” (3). Others see it as a “freedom of speech issue...If somebody wants to post something on a group or on their wall, I don’t think [the company] has a right to step in and say you can’t say anything negative about us” (12).

While respondents recognize that their younger employees have a different perspective on network privacy, they do not share it or endorse it. For example, there are respondents who believe that “work life and home life are very much intertwined” (13). For example, one respondent would expect to have access to a job applicant’s Facebook page and if this was not allowed, he would wonder “what do you have on there?” (5) Similarly, if something is discovered about someone’s posting on Facebook that is deemed to be inappropriate, a company “would take swift action, if we ever became aware of it” (16). Still, others qualify the extension of the business code of conduct beyond 9 to 5 to “business-related functions” (16) only.

From the responses of our interviewees, it appears that there is little agreement about an appropriate work life personal life boundary. “It is much more difficult to establish and pinpoint a line as to what is acceptable and what is not” (16). Because of the lack of clarity about the boundary, it is very difficult to develop a policy that is fair to employees, meets a company’s objectives and is ultimately able to be implemented.
Recruitment and Selection: Human Resources Use of Online Social Networks

Respondents were asked to describe the current and proposed use of OSNs to assist with the human resources functions of recruitment and selection of candidates for positions. None of the respondents reports a strategic and targeted use of OSNs for recruitment. However, there are certainly isolated instances of its being used both for certain positions and for informal recruiting by those already on Facebook. For example, one technique is to set up a Facebook space and provide information to prospective applicants on “what it would be like to work at the company and an opportunity to ask questions of recruiters” (2).

Although none of our respondents is using this technique extensively, there is a recognition by most of its power and importance. “You are trying to draw in younger employees in a way that is more consistent with the culture and way they use the Internet” (2). “Maybe when our management population gets younger and more attached to these networks, then maybe there will be more of it, but I think right now, it is not something we plan to address, but it is something we have at the back of our mind” (7). “This is one of those new methods of communicating and reaching out to a potential pool of candidates, especially for some of our entry level positions, which are a younger demographic” (10). In contrast, one respondent sees it “as the equivalent of wanting a fish and you go to the end of a pier and you put a line into it. Whatever bites, bites. You can get much more efficient than that” (4).

Another Human Resource application of Facebook is for screening and selection. Certainly “googling” a prospective candidate is done by a number of our respondents, although it is not accepted practice across all companies. Two respondents mention ethical concerns about getting access to information that may have been presumed to be private as well as concerns about mistaken identity and conclusions that may be drawn from erroneous material. Others maintain that as long as the request for access is transparent and upfront then access to OSN information is no worse than other background checks which may be part of the traditional selection process. Respondents admit, that “if we saw something negative on Facebook [about a job applicant], it would be factored into the hiring decision” (13).

There have been no documented complaints from unsuccessful candidates who believe they have been turned down because of what is posted on their Facebook page.

In general, OSNs may have potential for recruitment, but at this time probably only for the younger demographic and for entry-level positions. In terms of using the information posted to gain insight into the character of the potential hire, there is no agreement among respondents about whether that is an ethical and appropriate use of technology as well as whether the information would ultimately provide any insight into job performance. Once again, the
comments of respondents indicate that they see OSN as something very significant with the potential to impact how they do business, but at the moment they cannot articulate what form those impacts will take.

**Marketing Application of Online Social Networks**

We asked respondents to describe the current and proposed use of OSNs for marketing purposes including the gathering and sharing of information about selected market segments, and the promotion of products and services to the organization’s target market.

None of the respondents knows of any instances in which their company is using data gathered from an OSN to learn more about a particular target market. In line with their perception of unrestricted OSN information as public and not private, respondents do not view such potential collection as contravening existing Canadian personal information protection legislation such as PIPEDA.

Respondents do recognize the potential uses of this tool to achieve marketing objectives, but have no clear tactics in mind at the moment. “We’re really struggling as to how to use these tools for good, so to speak and how to use them to market to our customers” (3). “We went through a strategic planning process and we discussed the growth of the Internet and the use of these types of networks by our next generation of purchasers, and there has been a discussion of placing ads in Facebook” (6).

A couple of companies have current Facebook sites, but these are mainly designed to provide non-product information or to collect feedback on current services. Only one company actively uses OSNs to recruit respondents for marketing research purposes, both focus groups and survey questionnaires.

One respondent provided an example of how another company (not part of this project) has developed an innovative use of Facebook. A person logs onto his/her Facebook page and can order coffee as a gift for a client through a link on his/her own page that clicks directly into the coffee giving service website.

There appears to be recognition that there is much marketing potential within OSNs, but the specifics of leveraging that potential have yet to be determined.
Potential Uses of Online Social Networks

Finally, respondents were asked to consider the future uses of OSNs in the context of their organization’s goals and objectives.

In terms of the future, some respondents see OSNs as “something we have to manage as opposed to use” (3). Others see it as part of a larger shift; “the power is definitely shifting to consumers” (2). Most respondents do not contemplate the use of an existing OSN such as Facebook for their proprietary purposes, but may consider the development of a similar communication platform in-house, under their control, and “behind the firewall”.

There is potential for governments to develop much stronger and broader-based grassroots engagement in policy development by using OSNs as a replacement for town halls and citizen meetings.

In terms of a specific organization, there is the belief that by understanding how a social network operates, one can identify the “hubs” in terms of information exchange, which is significant because the people who hold these positions are pivotal in rolling out new programs and assisting in the social change process.
Implications and Recommendations

There is a new digital divide, and it is characterized by a perception of network privacy that is unique to young Canadians, and that is largely incomprehensible to an older generation of executives and managers. Young Canadians have embraced OSNs, and Facebook in particular to an incredible degree – nine out of ten use Facebook to communicate on a regular basis. That level of technological penetration approaches those reached by the television and the telephone. It is quite telling, and indeed speaks to the existence of a digital divide, that the executives and managers who participated in our project, and who were therefore willing to discuss OSNs, are largely reluctant to communicate with others on such networks themselves.

Furthermore, while young Canadians are comfortable posting large amounts of personal and private information on OSNs, they do so while differentiating between destinations for this information. Friends, family and work are clearly three separate networks in their mind, and they present a different persona to each, and expect members of each network to remain separate from each other. Young Canadians are concerned about their network privacy – about the risk that their personal information, while quite freely shared and open to many within their network of friends, will end up in the hands of others, such as their family and managers, who may not be members of the same network.

Within this age group, concerns are significantly greater among women than they are among men. Put differently, women have a stronger sense of network privacy than men do. More surprisingly, but reinforcing the hypothesis that network privacy is indeed a unique perception of privacy and not the product of ignorance, young Canadians about to enter the workforce full-time, such as graduate students or students in their graduating year, do not have greater concerns about their personal information than do those individuals who are just over the age of majority. The perception of network privacy, in other words, does not decrease as exposure and awareness to new risks and responsibilities increases.

Organizations, by and large, refuse to accept such network privacy concerns as valid, and adhere to the traditional approach by which personal information that is to be kept private must not be disclosed in the first place, and that young Canadians must be educated about the implications of having their information posted on OSNs with few restrictions.

It is clear, however, that individuals are aware, even more than could be expected, of both the privacy policies of OSNs and the technological measures available to control access to personal information. Young Canadians are not technological Luddites, but are technologically savvy, savvier than the older generation they are in the process of replacing at work. While there may
be concerns about the manner in which the technological measures function, and indeed as to whether the technology is secure, young Canadians know about it and attempt to use it. Moreover, they have at their disposal an arsenal of software developed for security and information protection, which they deploy to block malicious attacks on their identity and data. These individuals believe they have control over their personal information, and believe they have taken the appropriate steps to limit access to their personal information. They therefore blame themselves as well as whomever accessed their personal information, when there are negative consequences.

Surprisingly, young Canadians do not hold OSNs responsible or accountable for their network privacy breaches. Although some scenarios suggest such possibilities to participants in our survey, they are firmly and consistently rejected. OSNs such as Facebook are viewed as conduits, channels or pipelines for information, similar to the manner in which telephone, cable or satellite television services are perceived. OSNs are viewed as enabling socializing in a manner similar to the way in which a golf club or a church enables socializing, but participants do not contemplate holding their OSN accountable for the dissemination of harmful information any more than they will contemplate holding their golf club responsible for the gossip of its members, or their telephone company accountable for the contents of conversations carried over the phone.

OSNs, of course, profit from the socialization of their users in a manner that offline social networks and traditional methods of communication do not, and we discuss below some possible policy implications as a result.

Recommendations for Organizations

As a result of the digital divide between young Canadians and the organizations in which they work, or are about to work in we are able to offer the following suggestions:

Explicit Policies

Although the term policy is somewhat vague, and can be used by different organizations to refer to a range of instruments covering guidelines, best practices and codes of conduct, organizations by and large believe that their existing instruments will suffice. Interestingly, those organizations that have experienced some form of employee misconduct are less sanguine, and well on the route to adopting or modifying their existing human resources tool.

---

Young Canadians clearly indicate that they are unaware of the workplace views of OSNs, and that existing policies are not very helpful in directing their behaviour around OSNs while working.

Organizations should develop clear rules and guidelines for the use of OSNs at work and at home by their employees, based on principles that employees will accept. Depending on the organization, this may amount to no more than a clear statement that existing rules apply to OSNs at well.

**Internal Guidelines**
Organizations are also uncertain whether to actively seek information online about their workers and customers, or whether they should remain passive. We suggest that where certain processes already work well, such as in the case of existing recruitment and selection processes, a decision be made not to collect additional personal information. Such a recommendation must be complemented by a suggestion as to the proper role of an organization once information it has not been actively seeking has been brought to its attention, for example by way of customer complaint. Organizations will of course always comply with legal and professional requirements, but where discretion exists we suggest that organizations refrain from acting on the basis of such knowledge. Such restraint will support the network privacy perception limiting personal information to its intended network.

**Marketing**
Although the attraction of OSNs as a treasure trove of consumer information is understandable, and of course cultivated by OSNs to generate their revenue, organizations are advised to tread cautiously. It does not appear that the information offered by OSNs such as Facebook for commercial advertising purposes to organizations is in violation of PIPEDA or other provincial legislation, but it does appear to violate in most cases the targeted individual’s sense of network privacy. Some young Canadians welcome targeted advertising over the traditional mass-marketing approach, but they do so explicitly, and on their own terms. They wish to choose which persona to present to marketers, and which marketers to include within their network for such purposes.

**Education and Awareness**
We suggest that organizations educate themselves about the perceptions and concerns of young Canadians. Many managers and executives who participated in this project perceive what we call the digital divide to be a false one, or one that can be easily bridged by educating new and young employees about the risks of online socializing and the repercussions brought about through the indiscriminate sharing of personal information. This study suggests that the
apparent paradox of young Canadians behaving carelessly and in a risk-prone manner online, despite their perceived knowledge of privacy risks, is partially the result of their unique sense of network privacy. Organizations may be better served by seeking to understand and leverage this unique notion, rather than simply ignoring it, blocking it, or solely attempting to educate young Canadians about this notion’s risks. Changing the behaviour of young Canadians, to reduce their vulnerability on OSNs, will require an integrated and collaborative strategy comparable to what we see in other crime and safety prevention campaigns. This is particularly important as the business sector embarks on the recruitment of the young generation as employees and develops strategies to retain them as customers.

**Recommendations for the OPC**

Privacy Commissioners in Canada and other countries are uncertain as to the role they should play, if at all, in the regulation of OSNs and education of the public. Certain Commissioners take the position that there is an education and advocacy role for their office to play, but perhaps not a regulatory one; other Commissioners do not view OSNs and particularly the conduct of OSN users as one that deserves special attention or protection on their behalf. Based on our report, we suggest the following to the OPC:

**Public Education and Outreach**

The OPC has already been active in educating individuals about online conduct, and to a large degree it appears its message, and the message of other Privacy Commissioner and public advocacy groups, has reached its target. Young Canadians are aware of OSN privacy policies and attempt to control the dissemination of their personal information with tools provided by OSNs. Awareness levels could be improved, however, and more importantly, there is some evidence to suggest that, with online social networking, as with other risky behaviours, awareness does not necessarily translate into appropriate action.

Further research is needed to explore ways in which the privacy commissions can shape the perception and behaviours of young Canadians. For example, it is clear from the study that there is a need to clarify that such a notion of privacy cannot on the whole be protected satisfactorily online, and that network privacy breaches, when they do occur, are largely irreversible. At the same time, the OPC can and should educate young Canadians on the proper role of OSNs in such matters, as well as to request that OSNs change some of their practices, as we now discuss.
OSNs and PIPEDA
On the whole, OSNs are not in violation of PIPEDA and therefore we do not suggest that the OPC has any formal obligations in this matter. However, while it appears OSNs are not in violation of the letter of PIPEDA, they may well be in violation of its spirit, once the network privacy perception of the majority of their users is taken into account. Consider for example the controversy that erupted by the introduction of Facebook Beacon in 2007,\(^{17}\) a paradigmatic example of network privacy breach, while not apparently in violation of Canadian personal information protection legislation. We suggest that the OPC work with OSNs to ensure that users enjoy the measure of network privacy that they expect and desire, and that those users who wish to use OSNs, primarily if not solely, for the purpose of socializing with their friends be allowed to do so in an unfettered manner. In addition, the OPC must continue to track developments with OSNs and to develop appropriate mechanisms to ensure that the privacy of Canadians is appropriately protected.

Network Privacy Breaches
While young Canadians do not hold OSNs responsible for such breaches, it is clear to us that OSNs are best positioned to assist in the mitigation of, if not entirely eliminate, such breaches in their aftermath. Specifically, scenarios perceived as realistic by many young Canadians, in which their network privacy and reputation are harmed by the unsanctioned dissemination of their personal information by former friends and anonymous users, can easily be countered by OSNs. Facebook, for example, offers only limited assistance to individuals concerned about network privacy breaches, and does not assume any legal obligation in this matter under its terms of use. It is imperative to realize that OSNs can assist individuals by providing identifying information about anonymous users, or by removing information from the network, with minimal effort, and at a minimal cost. Litigation is not an affordable measure for many young Canadians in such circumstances, nor is it the most efficient. The OPC should advocate that OSNs assume greater responsibility for such breaches.

Appendix A
Quantitative Instrument

SCREENING QUESTIONS (DO NOT INPUT INTO SPSS FILE)

a) Are you a full-time student at Ryerson?

Yes  **CONTINUE
No  *THANK AND TERMINATE

b) In what School or Program are you currently registered?

IDENTIFY SCHOOL OR PROGRAM ON YOUR LIST AND ENSURE RESPONDENT IS PART OF YOUR ASSIGNED GROUP AND CONTINUE. IF NOT, *THANK AND TERMINATE.

c) Are you or have you ever been a registered member of an OSN (such as Facebook, MySpace or some other network)?

Yes  **CONTINUE
No  *Could you tell me why not? THANK AND TERMINATE

*KEEP A COUNT OF THE NUMBER OF STUDENTS FROM ALL THOSE WHOM YOU ASKED TO PARTICIPATE BUT WHO DID NOT MEET THE SCREENING CRITERIA OF BEING A MEMBER OF AN ONLINE SOCIAL NETWORK, INCLUDING ANY COMMENTS THEY OFFERED FOR THE LAST QUESTION.

**If all screening questions meet THE requirements for subject participation, hand Respondent the survey for self-completion.
Thank you for agreeing to participate in this survey!

SECTION A: The first questions relate to your use of the Internet and various online networks.

2. On average, how often do you use each of the following? (Check the box that best describes your usage)

<table>
<thead>
<tr>
<th>Network</th>
<th>6 - 7 days per week</th>
<th>1 - 5 days per week</th>
<th>1 - 3 days per month</th>
<th>Less than once per month</th>
<th>Never</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) E-mail</td>
<td>□5</td>
<td>□4</td>
<td>□3</td>
<td>□2</td>
<td>□1</td>
<td>□0</td>
</tr>
<tr>
<td>b) Instant Messengers</td>
<td>□5</td>
<td>□4</td>
<td>□3</td>
<td>□2</td>
<td>□1</td>
<td>□0</td>
</tr>
<tr>
<td>c) Chat rooms</td>
<td>□5</td>
<td>□4</td>
<td>□3</td>
<td>□2</td>
<td>□1</td>
<td>□0</td>
</tr>
<tr>
<td>d) Listservs</td>
<td>□5</td>
<td>□4</td>
<td>□3</td>
<td>□2</td>
<td>□1</td>
<td>□0</td>
</tr>
<tr>
<td>e) Bulletin Boards</td>
<td>□5</td>
<td>□4</td>
<td>□3</td>
<td>□2</td>
<td>□1</td>
<td>□0</td>
</tr>
<tr>
<td>f) Blogs</td>
<td>□5</td>
<td>□4</td>
<td>□3</td>
<td>□2</td>
<td>□1</td>
<td>□0</td>
</tr>
<tr>
<td>g) Online Social Networks</td>
<td>□5</td>
<td>□4</td>
<td>□3</td>
<td>□2</td>
<td>□1</td>
<td>□0</td>
</tr>
</tbody>
</table>

3. Which of the networks listed below you have heard about? (Check all that apply)

<table>
<thead>
<tr>
<th>Network</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) MySpace</td>
<td>□1</td>
</tr>
<tr>
<td>b) Facebook</td>
<td>□1</td>
</tr>
<tr>
<td>c) LinkedIn</td>
<td>□1</td>
</tr>
<tr>
<td>d) Windows LiveSpaces</td>
<td>□1</td>
</tr>
<tr>
<td>e) Other (specify)</td>
<td>□1</td>
</tr>
</tbody>
</table>

4. Which networks are you a member of? (Check all that apply)

<table>
<thead>
<tr>
<th>Network</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) MySpace</td>
<td>□1</td>
</tr>
<tr>
<td>b) Facebook</td>
<td>□1</td>
</tr>
<tr>
<td>c) LinkedIn</td>
<td>□1</td>
</tr>
<tr>
<td>d) Windows LiveSpaces</td>
<td>□1</td>
</tr>
<tr>
<td>e) Other (specify)</td>
<td>□1</td>
</tr>
</tbody>
</table>

5. Of the networks you belong to, which one is your MOST preferred? (Check only ONE)

<table>
<thead>
<tr>
<th>Network</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) MySpace</td>
<td>□1</td>
</tr>
<tr>
<td>b) Facebook</td>
<td>□1</td>
</tr>
<tr>
<td>c) LinkedIn</td>
<td>□1</td>
</tr>
<tr>
<td>d) Windows LiveSpaces</td>
<td>□1</td>
</tr>
<tr>
<td>e) Other (specify)</td>
<td>□1</td>
</tr>
</tbody>
</table>
SECTION B: Please relate your answers specifically to the online social network you identified as your MOST preferred network.

6. On average, how often do you log on to your most preferred network? (Check one)

- ☐ 1  More than once a day
- ☐ 2  Once a day
- ☐ 3  From 2 to 6 times a week
- ☐ 4  Once a week
- ☐ 5  Less than once a week

7. Which of the following pieces of information have you included on your social network profile? (Check all that apply)

- ☐ 1  a) My full real name
- ☐ 1  b) Only part of my real name
- ☐ 1  c) Only my nickname
- ☐ 1  d) Only a fake/joke name
- ☐ 1  e) A portrait photo of myself
- ☐ 1  f) A group photo that includes me in it
- ☐ 1  g) A joke/fake photo to represent me
- ☐ 1  h) My political preferences
- ☐ 1  i) My employer
- ☐ 1  j) My class schedule
- ☐ 1  k) My home town
- ☐ 1  l) My full address
- ☐ 1  m) My telephone number
- ☐ 1  n) My high school
- ☐ 1  o) My dating interests
- ☐ 1  p) My relationship status
- ☐ 1  q) My relationship partner’s name
- ☐ 1  r) My interests/hobbies
- ☐ 1  s) My favourite music, books or movies
- ☐ 1  t) Other (please specify) __________________________

8. On a scale of 1 to 5 where 1 is not at all concerned and 5 is very concerned, how concerned would you be if the following groups of people accessed your social network profile information listed above? (Circle the number that best describes your level of concern)

<table>
<thead>
<tr>
<th>Not at all Concerned</th>
<th>Very Concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>a) My friends</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>b) My parents</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>c) Other members of my family</td>
<td>1 2 3 4 5</td>
</tr>
</tbody>
</table>
d) My employer

e) People I don’t know

9. Which of the following statements relate to your experience with your preferred social network? (Check as many as apply)
   □1 a) I have read the privacy policy associated with my online social network.
   □1 b) I understand the terms of my online social network’s privacy policy.
   □1 c) I have adjusted my privacy settings to restrict some groups of people from accessing me online.
   □1 d) I use the default privacy settings set by the developers of my social network.
   □1 e) I have blocked specific people from accessing my online profile.
   □1 f) People I don’t know have tried to con me into letting them get access to my network.
   □1 g) I have reported content that I found distasteful or disturbing to the developers of the network.

SECTION C: The next few pages present five different scenarios that may happen on a social network site. Please read each one and answer the questions that follow, assuming you are the person involved.

Scenario 1:
You have just broken up with your significant other. You are shocked to see that the day after the breakup, your previous significant other posted compromising and what you thought were very private pictures of you on the social network. In addition, this person posted nasty comments that painted a very negative picture of you as a person. As a result, some people whom you thought were your friends have dropped you and you are no longer included in social events.

10. Which of the following best represents your experience with the scenario described above? (Check only ONE)
   □1 Something like this has happened to me.
   □2 Something like this has not happened to me, but it has happened to someone I know personally.
   □3 Something like this has not happened to me or to someone I know personally, but I have heard about it happening to others.
   □4 I have not heard of this happening.
11. Putting yourself into this scenario, on a scale of 1 to 5 where 1 does not reflect your views at all and 5 reflects them very well, please indicate how well each of the following statements reflects your views about who is responsible for your being dropped by people you thought were your friends and no longer being included in social events? *(Circle the number that best describes your view).*

<table>
<thead>
<tr>
<th>Options</th>
<th>Does not reflect views</th>
<th>Reflects very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) I am responsible</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>b) The person who posted the content is responsible</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>c) The people whom I thought were my friends are responsible.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>d) The developers of the network are responsible for allowing this material to be posted.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>e) Somebody else is responsible (please specify)</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
</tbody>
</table>

12. On a scale of 1 to 5 where 1 does not reflect your views at all, and 5 reflects your views very well, please indicate how well each of the following statements reflects your views on the issues identified in the scenario you have just read. *(Circle the number that best describes your view)*

<table>
<thead>
<tr>
<th>Options</th>
<th>Does not reflect views</th>
<th>Reflects very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) I get more upset about someone posting nasty comments about me than I do about someone posting compromising pictures of me.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>b) If this happened to me, in the future, I would be much more careful about who was taking pictures of me.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>c) If this happened to me, in the future, I would be much more careful about how I treated other people.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>d) I see myself as someone who takes the appropriate steps to limit who has access to my profile.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>e) It concerns me that material posted about me on the network does not always originate with me.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
</tbody>
</table>
f) No real harm can come from this kind of prank. 1 2 3 4 5

Scenario 2:
It was your birthday and you went out with friends for a night on the town. You had a wonderful time, drank way too much and really can’t remember most of the evening. The next day you see pictures of your escapades posted on one of your friend’s pages and tagged to you. Your family members see these pictures, are very upset with you and say they can no longer trust you.

13. Which of the following best represents your experience with the scenario described above? (Check only ONE)

☐ 1 Something like this has happened to me.
☐ 2 Something like this has not happened to me, but it has happened to someone I know personally.
☐ 3 Something like this has not happened to me or to someone I know personally, but I have heard about it happening to others.
☐ 4 I have not heard of this happening.

14. Putting yourself into this scenario, on a scale of 1 to 5 where 1 does not reflect your views at all and 5 reflects them very well, please indicate how well each of the following statements reflects your views about who is responsible for your family’s being upset and no longer trusting you? (Circle the number that best describes your view).

<table>
<thead>
<tr>
<th>Statement</th>
<th>Does not reflect views</th>
<th>Reflects very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) I am responsible</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>b) The person who posted the content is responsible</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>c) My family members are responsible, as they shouldn’t have been checking up on me.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>d) The developers of the network are responsible for allowing this material to be posted.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>e) Somebody else is responsible (please specify)</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
</tbody>
</table>

15. On a scale of 1 to 5 where 1 does not reflect your views at all, and 5 reflects your views very well, please indicate how well each of the following statements reflects your views on
the issues identified in the scenario you have just read. (*Circle the number that best describes your view*)

<table>
<thead>
<tr>
<th>a) I get more upset about my family seeing compromising pictures of me than if acquaintances see them.</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>b) It is not right when people can have access to information that was not intended for them.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>c) If this happened to me, in the future, I would be much more careful about how I behaved in public.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>d) I use the social network to keep track of my siblings or relatives to make sure they are not doing something they shouldn’t do.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>e) No real harm can come from this kind of prank.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Scenario 3:
Anonymous comments circulate on the online social network about your having been arrested for shoplifting. This is not true and you are shocked to see that these comments have made the rounds to all your friends. No matter what you say, everyone believes you are a shoplifter.

16. Which of the following best represents your experience with the scenario described above? (*Check only ONE*)

- [ ] 1 Something like this has happened to me.
- [ ] 2 Something like this has not happened to me, but it has happened to someone I know personally.
- [ ] 3 Something like this has not happened to me or to someone I know personally, but I have heard about it happening to others.
- [ ] 4 I have not heard of this happening.

17. Putting yourself into this scenario, on a scale of 1 to 5 where 1 does not reflect your views at all and 5 reflects them very well, please indicate how well each of the following statements reflects your views about who is responsible for your friends’ believing that you are a shoplifter? (*Circle the number that best describes your view.*)
18. On a scale of 1 to 5 where 1 does not reflect your views at all, and 5 reflects your views very well, please indicate how well each of the following statements reflects your views on the issues identified in the scenario you have just read. *(Circle the number that best describes your view)*

<table>
<thead>
<tr>
<th>Does not reflect views</th>
<th>Reflects very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) I am responsible</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>b) The person who posted the content is responsible</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>c) The people whom I thought were my friends are responsible</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>d) The developers of the network are responsible for allowing this material to be posted.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>e) Somebody else is responsible (please specify)</td>
<td>1 2 3 4 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does not reflect views</th>
<th>Reflects very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) I should be able to count on the network developers to put a stop to this.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>b) Situations like this make me feel really helpless about protecting myself and my character.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>c) No real harm can come from this kind of prank.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>d) I believe I am able to take the appropriate steps to control what is posted about me on my social network.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>e) In instances like this, the developers of the social network should tell me the name of the person who is posting these lies about me.</td>
<td>1 2 3 4 5</td>
</tr>
</tbody>
</table>
Scenario 4:
You called in sick to work, because you really wanted to go to your friend’s all day graduation party. The next day you see several pictures of you having a great time at the party. Because the pictures are dated, you start to worry about whether you might be caught in your lie about being sick. You contact the developers of the social network and ask that the pictures be taken down because the tagging goes so far, it would take you too long to find all the pictures. There was no response from the network. You are stunned to be called in by your supervisor a week later to be advised that you were being “written up” for taking advantage of sick leave and put on notice that if it happened again you would be terminated.

19. Which of the following best represents your experience with the scenario described above? (Check only ONE)
□ 1 Something like this has happened to me.
□ 2 Something like this has not happened to me, but it has happened to someone I know personally.
□ 3 Something like this has not happened to me or to someone I know personally, but I have heard about it happening to others.
□ 4 I have not heard of this happening.

20. Putting yourself into this scenario, on a scale of 1 to 5 where 1 does not reflect your views at all and 5 reflects them very well, please indicate how well each of the following statements reflects your views about who is responsible for your being written up by the supervisor and threatened with termination? (Circle the number that best describes your view).

<table>
<thead>
<tr>
<th></th>
<th>Does not reflect views</th>
<th>Reflects very well</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Views at all well</td>
<td></td>
</tr>
<tr>
<td>a) I am responsible</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>b) The person who posted the content is responsible</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>c) My supervisor is responsible – he/she shouldn’t have been checking up on me.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>d) The developers of the network are responsible for allowing this material to be posted.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>e) Somebody else is responsible (please specify)</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
</tbody>
</table>

87
21. On a scale of 1 to 5 where 1 does not reflect your views at all, and 5 reflects your views very well, please indicate how well each of the following statements reflects your views on the issues identified in the scenario you have just read. (Circle the number that best describes your view)

<table>
<thead>
<tr>
<th></th>
<th>Does not reflect views</th>
<th>Reflects views very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) It is not right when people can have access to information that was not intended for them.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>b) No real harm can come from this kind of prank.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>c) It concerns me that material posted about me on the network does not always originate with me.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>d) The developers of the online network should have responded to my request immediately.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>e) If I had been terminated, the developers of the online social network should have been held legally responsible.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
</tbody>
</table>

**Scenario 5:**
In this scenario, assume that you are a manager with five employees. You are in your early thirties and your employees are in their twenties.

22. On a scale of 1 to 5 where 1 is not appropriate and 5 is very appropriate, how appropriate would it be for you (as the manager) to: (Circle the number that best describes your view)

<table>
<thead>
<tr>
<th></th>
<th>Not Very Appropriate</th>
<th>Appropriate</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Use a social network to check up on what your employees do during their personal time without them knowing.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>b) Require your employees to add you as a ‘friend’ to their social network.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>c) Use a social network to check out the character of someone who has applied for a job.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>d) Proactively research social networks to identify potential high quality candidates for future positions.</td>
<td>1 2 3 4 5</td>
<td></td>
</tr>
</tbody>
</table>
23. On a scale of 1 to 5 where 1 is strongly disagree and 5 is strongly agree, please give your level of agreement or disagreement with the following statements. Remember to answer as if you were the manager with the five employees. (*Circle the number that best describes your view*)

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>e) Socialize with your employees after work hours through a social network.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f) Promote goods and services made by your company to network users.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| a) Accessing online social networks should not be allowed during work hours. | 1 | 2 | 3 | 4 | 5 |
| b) A person wanting to move up the career ladder should not be part of online social networks because you can’t completely control what is posted about you. | 1 | 2 | 3 | 4 | 5 |
| c) Work life is completely separate from personal life and what you do in one should not affect the other. | 1 | 2 | 3 | 4 | 5 |
| d) Knowing how a person behaves outside of work hours gives managers insight into whether that person is ready for a promotion. | 1 | 2 | 3 | 4 | 5 |
| e) A smart manager will use online social networks to learn more about the company’s customers. | 1 | 2 | 3 | 4 | 5 |
| f) Online social networks are becoming significant marketing tools for companies to promote their goods and services | 1 | 2 | 3 | 4 | 5 |
**SECTION D: If you have worked, either full or part-time, at any time during the past twelve months, please answer the following questions. Otherwise, please skip this section and go to SECTION E.**

24. In your most recent workplace:

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Is your immediate supervisor a member of your online social network?</td>
<td>☐ 1</td>
<td>☐ 2</td>
<td>☐ 3</td>
</tr>
<tr>
<td>b) Has your immediate supervisor asked to be added to your online social network?</td>
<td>☐ 1</td>
<td>☐ 2</td>
<td>☐ 3</td>
</tr>
<tr>
<td>c) Is any senior executive of the company you work for (above your immediate supervisor) a member of your online social network?</td>
<td>☐ 1</td>
<td>☐ 2</td>
<td>☐ 3</td>
</tr>
<tr>
<td>d) Has any senior executive asked to be added to your online social network?</td>
<td>☐ 1</td>
<td>☐ 2</td>
<td>☐ 3</td>
</tr>
<tr>
<td>e) Has your workplace encouraged the use of an online social network for work related purposes?</td>
<td>☐ 1</td>
<td>☐ 2</td>
<td>☐ 3</td>
</tr>
<tr>
<td>f) Does your workplace have a formal policy related to the use of online social networks during company time?</td>
<td>☐ 1</td>
<td>☐ 2</td>
<td>☐ 3</td>
</tr>
<tr>
<td>g) If there is a policy, does it forbid all use of social networks during company time?</td>
<td>☐ 1</td>
<td>☐ 2</td>
<td>☐ 3</td>
</tr>
<tr>
<td>h) If there is a policy that forbids all use of online social networks during work time, do employees generally abide by the policy?</td>
<td>☐ 1</td>
<td>☐ 2</td>
<td>☐ 3</td>
</tr>
<tr>
<td>i) What is the policy? <em>(Please specify)</em></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SECTION E: Please complete the next two sentences with your own thoughts:

25. With respect to my personal life, the thing that worries me most about being on an online social network is...

___________________________________________________________________________

___________________________________________________________________________

26. With respect to my work life, the thing that worries me most about being on an online social network is...

___________________________________________________________________________

___________________________________________________________________________
SECTION F: The final few questions are for grouping purposes only.

27. In what Faculty are you currently registered?

☐ 1 Faculty of Arts
☐ 2 Faculty of Communication and Design
☐ 3 Faculty of Community Services
☐ 4 Faculty of Engineering and Applied Science
☐ 5 Ted Rogers School of Management

28. In what year are most of your courses?

☐ 1 First
☐ 2 Second
☐ 3 Third
☐ 4 Fourth

29. In an average week, about how many hours are you employed in a paying job?

☐ 1 None
☐ 2 Less than 10
☐ 3 10-14
☐ 4 15-19
☐ 5 20-24
☐ 6 25 or more

30. Are you:

☐ 1 Male
☐ 2 Female

31. How old are you? _____________

THANK YOU FOR YOUR TIME AND COOPERATION!

(Group and Respondent Number are to be completed by the interviewer:)

GROUP NUMBER _____________   RESPONDENT NUMBER ___________
Appendix B
INTERVIEW SCHEDULE
A) GENERAL
1. What online social networks are you aware of/do you use?
2. If familiar with Facebook, then
   • How did you first hear about it?
   • What do you use it for?
   • Are your co-workers Facebook friends? Your employees? Your family? External to work friends?
   • Describe your feelings towards sharing your personal information on Facebook to others on your friends list.
3. Are online social networks beneficial to your work life? If yes, how so?

B) CORPORATE POLICIES / PRACTICES
1. What are your organization’s policies on online social networks? (e.g., usage at the workplace, how content is used)
   • Does your organization have a position on online social networks (e.g., encourage, ignore, prohibit)
   • Does your organization have any disciplinary policies regarding usage/over-usage of online social networks during work hours or using work equipment?
   • Does your organization have any disciplinary policies regarding posting or viewing of unsuitable or inappropriate materials during work hours or using work equipment?
2. If your organization has a “work network” on Facebook:
   • How/Why was it established?
   • Are employees actively encouraged to join the network? If so, how?
   • In what ways, if any, does having a “work network” on Facebook impact employees?
3. If your organization does NOT have “work network” on Facebook:
   • Why does your organization not have a “work network” on Facebook?
   • In what ways, if any, does having a “work network” on Facebook impact employees?
4. In what ways, if any, have online social networks positively impacted workplace activities? (e.g., productivity, social connection & teambuilding)
5. In what ways, if any, have online social networks negatively impacted workplace activities? (e.g., office politics, distraction)
6. What worker confidentiality concerns arise when employees use online social networks?
   • Have there been employee concerns that activity on online social networks would impact their careers? If so, how have the concerns been addressed?
• How would compromising details found on an employee’s profile page affect him/her in the workplace?

7. If an employee of your company identifies on their page that they work for you, does that concern you?
   • Are there any specific policies to censor/discourage information posted on an employee who has identified that profile pages?
   • Would you possibly take any action or impose guidelines if the employee (who identified themselves as working for you on their page) posted content that could be harmful to the company’s reputation? (e.g., disclosure of confidential or sensitive company information, employee misconduct, negative comments about the company).

8. How do you feel about the work life and personal life division of online social networks? (e.g., managers and employee interactions on OSN)

C) RECRUITMENT & SELECTION (consult with HR if necessary)
1. Do you/would you utilize online social networks to research applicants (internal or external)?
2. Would the possession of an active online profile be considered a positive, negative, or neutral to applicants (internal or external). Why?
3. Would you post jobs or accept applications over online social network? Why/why not?
4. Have there been employee concerns that activity on online social networks would impact their applications? If so, how have the concerns been addressed?

D) MARKETING (consult with Marketing if necessary)
1. In what ways, if any, can the gathering and sharing of information on online social networks help your organization?
   • Does your organization participate in collecting information on online social networks?
2. In what ways, if any, can the utilities offered by online social networks help your organization? (e.g., groups, forums)
   • Does your organization manage any utilities? (e.g., groups, forums)
3. In what ways, if any, can the marketing aspect of online social networks help your organization (e.g., public relations, advertising, promotional)?

CONCLUDING QUESTIONS:
1. Do you have any further comments on online social networks as a potential tool for your organization?
2. Do you have any further comments on online social networks as a disadvantage to your organization?
3. Would you be interested in learning more about online social network and how it can be incorporated to your organization? Which aspects?