



Research Report

Focus Testing Privacy Issues and Potential Risks of Social Networking Sites

Office of the Privacy Commissioner of Canada

March 20, 2009

Proprietary Warning

The information contained herein is proprietary to the Office of the Privacy Commissioner and may not be used, reproduced or disclosed to others except as specifically permitted in writing by the originator of the information. The recipient of this information, by its retention and use, agrees to protect the same and the information contained therein from loss, theft or compromise. Any material or information provided by Office of the Privacy Commissioner and all data collected by Decima Research Inc. will be treated as confidential by Decima Research Inc. and will be stored securely while on Decima Research Inc. premise (adhering to industry standards and applicable laws).

Toronto

2345 Yonge Street
Suite 405
Toronto, Ontario
M4P 2E5

t: (416) 962-2013
f: (416) 962-0505

Ottawa

160 Elgin Street
Suite 1820
Ottawa, Ontario
K2P 2P7

t: (613) 230-2200
f: (613) 230-9048

Montreal

1080 Beaver Hall Hill
Suite 400
Montreal, Quebec
H2Z 1S8

t: (514) 288-0037
f: (514) 288-0138

Vancouver

666 Burrard Street
Suite 500
Vancouver, British Columbia
V6C 3P6

t: (778) 370-1373
f: (604) 601-2074

www.decima.com

info@decima.com



Table of Contents

Introduction	1
Executive Summary	3
Résumé.....	Error! Bookmark not defined.
Social Networking Website Usage	6
Social Networking Website Experiences.....	10
Opinions on Online Privacy in General	12
Online Privacy and Social Networking Websites.....	14
Interest in Further Information.....	17
Appendix A: Recruitment Screeners	172
Appendix B: Moderators Guide	17

Introduction

Decima Research is pleased to present this report to the Office of the Privacy Commissioner of Canada (OPC) based on qualitative research to gather Canadians' insights on privacy issues and potential risks of social networking sites.

Background and Objectives

The ubiquity of the internet as a platform for communications continues to raise issues of privacy for users. With the advance of community building technologies such as social networking sites, there has arguably been a rise in concern for personal privacy. The Office of the Privacy Commissioner has received many inquiries regarding privacy issues and potential risks associated with collecting personal information, particularly on social networking sites such as Facebook.

Given that social networking is a relatively recent phenomenon, it is important for OPC to more thoroughly understand how Canadians perceive these kinds of sites and the privacy issues and risks that surround its use. In particular, understanding how those who are the most frequent users of these sites think about these questions and understand what rules are (and are not) in the realm of privacy is important to understand in regard to shaping new policy.

As a result, the OPC was interested in conducting focus groups in various cities across Canada to gain insight on privacy concerns among users of social networking sites. The findings presented in this document will provide guidance to the OPC and will help the organization further develop work in this area.

The findings below are based on eight focus groups held in Ottawa (4), Winnipeg (2) and Montreal (2) between December 15th and 17th, 2008. Each focus group was approximately 2 hours long and had an average of 8 people in attendance. A screening process was used to ensure groups were a good mix of gender, income and internet use habits.

All participants were users of at least one social networking website.

Appended to this report are the screener and moderator's guide used in this study.

The groups were segmented by age and language as explained in the table below:

	Late teens/ Early twenties	Late twenties/ Thirties	English	French	Dates
Winnipeg (2)	1	1	2		Dec. 16, 2008
Ottawa (4)	2	2	3	1	Dec. 14-15, 2008
Montreal (2)	1	1		2	Dec. 16, 2008

Executive Summary

Decima Research is pleased to present this report to the Office of the Privacy Commissioner of Canada (OPC) based on qualitative research to gather Canadians' insights on privacy issues and potential risks of social networking sites.

In order for the OPC to more thoroughly understand how Canadians perceive social networking sites and the privacy issues and risks that surround their use, the OPC commissioned Decima Research to conduct focus groups in various cities across Canada to gain insight to this privacy issue, among users of social networking sites.

In total, eight focus groups were held across three cities between December 15th and 17th, 2008: Ottawa (4); Winnipeg (2); and Montreal (2). Each focus group was approximately 2 hours long and had an average of 8 people in attendance. Groups were divided by age with a focus on younger users and beyond that a screening process was used to ensure groups were a good mix of gender, income and internet use habits.

Key Findings

Participants indicated they use social networking sites – Facebook, primarily – on a regular basis. Fairly uniformly, participants said they are primarily using the site to keep in touch with friends. Very few of these current users could recount a negative experience because of using their social network site.

Nearly all participants had four particular activities in common:

- Post information or messages about themselves or their activities;
- Read information or messages of their friends;
- Browse pictures that friends or others post; and
- Post pictures.

Pictures are clearly a valuable, if not vital, element for most of the users we studied. When discussing the identification of people in photos:

- some had no reservations or concerns about any risks associated with posting photos and identifying those in them;

- some said they do not identify people in photos because they could not be bothered and appeared not to have considered the privacy risks of such activities; and
- some have avoided the practice for privacy-related reasons, with these reasons tending to be about avoiding negative social consequences rather than about avoiding any risk relating to personal information being compromised or inappropriately used.

Few of the participants indicated they had installed applications, but the discussions suggested that they had limited awareness of what variety of applications they must necessarily already be using – since the activities they described almost always require applications.

Generally, people did not indicate being very concerned about their personal privacy online – either in general, or specifically in terms of their activities on social networking sites. Nevertheless, most users did tend to indicate having taken steps specifically to reduce risks with these steps typically falling into one of two areas:

- consciously, pro-actively adjusting privacy settings to make their profiles accessible only to those whom they feel pose no degree of risk; and/or
- avoiding the posting of anything (i.e., messages, profile info or photos) that they deem as having a realistic chance of causing some difficulty in the future.

Fundamentally, their comfort level with their sense of exposure to risk related directly to the user-designated privacy settings they had established. The impression was that the privacy settings already in place on Facebook provide an adequate level of comfort and control over who can and cannot see their personal information. The older groups tended to feel that they had control over the information they put online and who has access to it, therefore their level of concern was mitigated by their own privacy management. Younger generations tended to describe taking fewer precautions and seemed less concerned with their privacy online in general.

Respondents all claimed to be aware of, and accepting of, Facebook using their personal information to target advertising to their users. When questioned about third parties having access to their information, many said they assumed this was happening and that was a reasonable cost.

Regardless of the site or service being accessed online, people typically indicated being comfortable revealing personal information online when

they feel that the benefits outweigh the risks. This is particularly true in specific cases (like online banking) where truly valuable information is being revealed but the user trusts that it is being kept secure.

The risk of economic impact was most often cited as the risk of greatest concern. When prompted for the greatest threats to personal privacy online, the participants tended to refer to conducting financial transactions online. Given that they do not undertake financial transactions as part of their activities on social networking sites, this activity was regarded as involving the transfer or provision of less potentially damaging information.

For social networking sites, the benefits (primarily of being able to stay in touch with friends easily and free of charge) were described as outweighing the risks (limited, low-value personal information being exploited in a harmful way).

Looking at some of the privacy policies of Facebook, the greatest concern appeared to be that applications force users to divulge not only their information but that of their friends as well. It was often described as unfair for others to sacrifice their own privacy for the benefit of a friend who wants to use an application.

Few participants said they had looked for information about privacy on social networking sites and none said they did so outside of the provider's website.

Participants did tend to recommend that social network providers be as clear and upfront as possible with users about what information will be used by whom and how it will be used.

Social Networking Website Usage

Preferred Sites and Typical Frequency

Most participants indicated they use social networking sites on a regular – basically daily – basis. For many, this meant an hour or more each day while for others it meant brief, sporadic visits during the course of a week.

Younger participants tended to describe spending more hours on social networking sites during each visit and doing so on a more frequent basis, compared to the older groups.

All of the participants were users of Facebook, with most saying it is their exclusive social networking site. Some claimed to use, have used, or heard of alternative sites such as Twitter and MySpace but Facebook prevailed as the social networking site of choice.

Typical Behaviour

As the name implies, a social network site is for socializing with friends, family and colleagues. These users appreciate the role that a site like Facebook plays for them in ensuring they are up-to-date on what their friends are up to.

Participants were probed on the specific types of activities they do when spending time on their social networking site. **Nearly all participants had four particular activities in common:**

- **Post information or messages about themselves or their activities;**
- **Read information or messages of their friends;**
- **Browse pictures that friends or others post; and**
- **Post pictures.**

Pictures are clearly a valuable, if not vital, element for most of the users we studied. Photos were appreciated for providing a richer experience. That being said, there appeared to be a relatively small group who were fairly adamant that they do not want a photo of themselves on their own page or on the pages of others. For some, their preferred approach to posting photos has been curtailed by the wishes of others in their lives (such as a spouse), who discourage the posting of their image or name or that of their children.

“Facebook is the only way we communicate now. All of my friends are on now and if they aren’t, they’re overlooked.”

“I don’t put photos up and I ask my friends not to put photos of me. I just don’t want my picture on the net.”

For those people who are less inclined to want photos posted, there was a discomfort with the idea of being visible, let alone visibly identified, on the Internet.

Tagging

All participants knew what being “tagged” meant and most were aware if they had been tagged in photos posted by others. Many indicated they have tagged people in photos they posted.

However, some participants pointed out they do not tag people in photos and cited one or both of two specific reasons for not doing so:

- “not worth the effort;”
- not interested in tagging; or
- the photo was unflattering or embarrassing and therefore, it would be unkind to identify the person in the photo.

This last reason is certainly related to respecting the privacy of one’s friends. However, some of these people who do not tag people in unflattering photos indicated they have tagged the same individual in a photo that was not unflattering. Therefore, even in some of these cases where tagging is avoided, privacy is consciously protected when it is felt there is a threat on a social level, rather than protecting privacy to reduce threats related to identity or personal information.

When discussing the instances of participants having been tagged in photos posted by others, although participants did not typically get asked for their approval, this action was never described as a grave concern. While perhaps embarrassing to some, this never emerged as a grave concern as respondents claimed this problem could be solved with a simple “un-tag” effort.

There was some variance in terms of who could see their pictures. Some had set their privacy settings so only their friends could see pictures, some had settings so only their friends and networks could see, others claimed their pictures were public and some could not recall. Some respondents went as far as asking their friends not to post pictures of them online.

Among the older participants, those who were parents tended to indicate having more restrictive policies in terms of what photos or identification of their children are posted.

Fundamentally, when it comes to photos with identification:

- some had no reservations or concerns about any risks associated with posting photos and identifying those in them;
- some could not be bothered and appeared not to have considered such risks;
- some avoided the practice for privacy-related reasons, with these reasons tending to be about avoiding negative social consequences rather than about avoiding any risk relating to personal information being compromised or inappropriately used.

Applications Used

On the topic of applications, participants were asked if they ever install them. **Given this particular prompting, only a relatively small group claimed to have installed applications.** The types of applications they cited as having installed varied from online games to applications in which user can send friends things such as alcoholic drinks.

However, given the activities indicated by most (i.e., posting photos) and the limited list of applications discussed when specifically prompted, it would appear that participants were not considering applications such as Facebook Photos to be an applications they installed. (photos isn't a separate and third party app) Thus, the discussion suggested that **there was only limited awareness of what variety of applications they must necessarily already be using.** (I think the observation is correct, but the reference to photos weakens the point)

Activities Avoided

Activities that were generally not done included:

- entering contests on Facebook – few were aware of them;
- using the gift function – at best, it appeared to have been a passing interest for some;
- accepting friend requests from people they don't know – receiving such requests was described as a rare occurrence that was usually a matter of failing to recall an acquaintance rather than a receiving a message from a complete stranger;
- look at people's profiles they don't know – some admitted to having done so, but typically this action was described a result of

seeing that person on a friend's page, rather than a random scan;
and

- sending out invitations for their friends to join social networking sites – the typical reason for not doing this was that “they are already there.”

Social Networking Website Experiences

Nature of Experiences

Given the fact that these participants were current users of a social networking service, it is not surprising that their experiences tend toward the positive rather than the negative. Indeed, it would have been more surprising to hear stories of people continuing to take advantage of it despite bad experiences. All the participants named Facebook as their preferred social networking service.

Consistently, participants named keeping in touch with friends as their most positive experience on, or benefit from, Facebook. Many told stories of reconnecting with long lost friends or people met while travelling and being easily able to stay in touch on Facebook despite vast distances and time zones separating them.

Among these current users, very few could recount a negative experience on Facebook. Some referenced having heard of experiences such as embarrassing photos or people being fired for saying or posting something bad about the employer.

“I feel I have a level of control over it”

When discussing negative experiences, there was a recurring theme expressed across all groups and age cohorts: users felt they had already taken steps to adequately reduce the personal risk posed by negative experiences.

The steps that users described having taken to reduce risks typically fell into one of two areas:

- **setting their profiles to be accessible only to those whom they feel pose no degree of risk; or**
- **not posting anything (i.e., messages, profile info or photos) that they deem as having a realistic chance of causing them some difficulty in the future.**

Although many described themselves as concerned about their privacy, they tended to feel fairly confident that they were not at risk based on the information they had posted or the settings they had established.

Probing more deeply into the kinds of personal information respondents put on their Facebook profile, many indicated posting information on where they live, their networks, their age, education and their birthday (although often excluding birth year) on their profiles.

“I don’t fill out interests, music; it’s just waste of space and time”

Some did not want to put up information such as interests and music for the mere reason that they didn’t want it cluttering their profile.

Fundamentally, the comfort level with the level of detail provided on the profile appeared directly related to the accessibility settings the user established. The more closed the community permitted to see the profile information, the higher level of comfort with providing greater detail.

“I put my cell phone on there so they can’t do a reverse lookup”

Respondents described themselves as less willing to put on their profile anything “too close to home.” Phone numbers and addresses were typical examples of information that was seen as representing too much exposure. For those who did put up such information, they generally had a reason for excusing it from privacy concerns, such as using a cell number which by nature, cannot be looked up in “reverse.”

Opinions on Online Privacy in General

Concern for Protecting Privacy

“[Facebook] is so easy; it’s totally worth the risk”

Generally, people were not very concerned about their personal privacy online. While many assumed bad things were happening such as identity theft or credit card circumvention, very few saw this as a deterrent to changing their online behaviour.

The older groups tended to feel that they had control over the information they put online and who has access to it, therefore their level of concern was mitigated by their own privacy management.

Younger generations tended to describe taking fewer precautions and seemed less concerned with their privacy online.

A trend that emerged across age groups was a general acquiescence that the information you put online is at risk of being used in a harmful way. When discussing this sentiment, many pointed out that without being able to cite an actual negative, harmful experience, one will default to continuing to feel the benefits of any specific online activity outweighs the risks.

“If they manage to get my credit card, it is all debt...they’d probably be doing me a favour”

Identity theft was something that came up in nearly every group. However, yet again, people either claimed credit card companies and banks are very good at taking care of such an infringement that it was really no concern for them. Some also claimed they either had no money or little to lose if someone were to steal their identity. Also, there was an underlying impression of people hearing about identity theft happening but there seemed to be little concern of it actually happening to them.

“The internet is a tool of our generation and yes, there are people out there trying to steal information but banks and credit card companies are doing a lot to stop it from happening”

Relative to other online activities and services, social networking sites rank fairly low in terms of level of concern and the relationship with willingness to partake. Activities that did evoke enough concern for participants to claim they avoid participation generally revolved around an activity in which credit card information was provided on behalf of the participant. Namely, eBay was a site that people were concerned about and not willing to partake. However, classified sites such as UsedOttawa, Craigslist or Kijiji evoked very little concern and people were quite willing to do it. The reasons given were generally that sites such as these allow the buyer to see the merchandise before they buy. Additionally, participants seemed to take comfort in the locality of this service, so much that some had let sellers come to their homes to deliver the merchandise.

Banking online was also brought up in many of the groups, particularly in the older cohorts. Most indicated they conduct banking online and while there was some level of concern given the economic risks attached, there was a general consensus that:

- banking online is so easy that the risks outweigh the benefits; and
- people took comfort in the “big name” aspect of their bank. It’s a name they can trust and if people’s financial information were being circumvented on a regular basis nobody would use the service.

Beyond banking, the “brand name” of the website provider was often mentioned as a key influence on willingness to provide information. Many mentioned that the company had a reputation to maintain, had invested ample resources in securing online information and some went further into saying that the brand name company would have more to lose if it ever let customer information fall into the wrong hands.

Conversely, participants tended to say they are less comfortable divulging personal information to individual sellers (i.e. eBay vendors), particularly those who are not based locally.

In sum, **people typically indicated being comfortable revealing personal information online when they feel that the benefits outweigh the risks, particularly in the specific cases (like online banking) where felt they are revealing truly valuable information but they trust that it is being kept secure.**

The risk of economic impact was most often cited as being of greatest concern. It was pervasive and tended to be the foundation for determining the degree of risk to which they felt exposed for any particular online activity.

Online Privacy and Social Networking Websites

Privacy Measures Taken by Users

Specifically on topic of privacy and social networking sites, **basically all participants claimed to be aware of privacy settings**, although some indicated having set no restrictions and being perfectly comfortable with that status.

Most claimed to have customized a privacy setting on their social networking page – typically, setting certain elements or all elements to “friends only” or “friends and networks.”

Very few participants regularly checked these settings to see if they have been changed or updated.

“I think it’s my job to control the disclosure of my personal information, I don’t trust [Facebook] to do it for me”

Some respondents had public profiles and some had profiles in which only their friends could see. Amid the younger groups there was a general complacency that the information one puts on Facebook is not harmful in any way. Many of the respondents took solace in the belief that their information is fairly unimportant or not valuable, and therefore expected no one to be using it or wanting it. Along similar lines, many claimed the information one puts up on a social networking site is public domain and take ownership of personal responsibility to maintain and manage information in order to reduce their risk.

Generally, the impression was that the privacy settings already in place on Facebook provide an adequate level of comfort and control over who can and cannot see their personal information.

It is worth noting that when discussing the privacy concerns relating to social networking sites, the conversation always defaulted to being about the information that can be seen by people who visit a user’s page – not the information provided to the social networking site for its own use. Some did augment the discussion by mentioning this aspect, but the overall view was that providing the “mandatory” information was a reasonable price to pay in exchange for using the service free of charge.

“If the info they’re taking is for statistical purposes to target marketing or even to help improve the site, that’s fine with me”

Information Used by Social Networking Sites

Respondents all claimed to be aware of Facebook using their personal information to target advertising to their users. Many referenced seeing ads that were tailored to them based on the information they put up on Facebook. However, again, many were

complacent based on the fact this was how most sites make money and because it doesn't really affect them in a negative way, they did not seem to be too concerned.

In terms of third parties having access to their information, many said they assumed this was happening and that was a reasonable cost – the cost primarily being targeted advertising and in some cases spam email attributed to the social network profile. Many saw this as a mere trade off for using a service they enjoy so much and it is just part of the risk of being online. Few volunteered any specific details on how it was being used or by whom.

When discussing the greatest threats, it tended to be about instances of conducting financial transactions online and given that they do not make a financial transaction at their social networking site, that activity was regarded as involving the transfer or provision of less potentially damaging information. Others indicated that they have nothing to lose at their young age and therefore, they felt the economic risk was non-existent.

For social networking sites, the benefits (primarily of being able to stay in touch with friends easily and free of charge) were described as outweighing the risks (limited, low-value personal information being exploited in a harmful way).

Transparency of Privacy Policies

When probed on whether they feel social networking sites should be more transparent about how they collect, use and protect personal information, many seemed content with the current level of disclosure and indicated being rather indifferent to the idea of disclosing further specifics into how their information is being used.

Very few of the participants had read much of the information contained in the privacy policies or user license agreements and described themselves as simply having clicked “accept” rather than making a judgment based on a thorough understanding of the agreement. That being said, some were familiar with details such as the sharing of information with third parties.

In each group, four conditions were read to participants from the Facebook privacy policy:

- Facebook collects your browser type and your IP address
- Facebook deems itself *not* responsible for circumvention of any privacy settings you stipulate

- Facebook uses information on your profile without identifying you to third parties
- Almost all applications you sign up for, you generally have to agree that the application developer has complete access to your profile information, photos, your friends' information and other content

Participants tended to have little reaction to any of these statements, with few showing concern.

That being said, some were disappointed with the notion that Facebook would not be responsible if the privacy settings it provided were circumvented. In many of these cases, the discussion resulted in a sense that if someone worked hard enough, any system, no matter how secure, could be infiltrated, but that did not mean it would be a likely occurrence.

“Even if I don’t use the applications, if one of my friends is, they get my information anyway!”

Perhaps **the statement that prompted the greatest concern was that applications force users to divulge not only their information but that of their friends as well.** A few claimed not to use applications for this very reason. Of those who were unaware of this fact, many felt it was unfair and over stepping boundaries.

In terms of the other policies mentioned, there was little concern and general agreement these are just the trade offs for using the service.

Interest in Further Information

Few participants said they had looked for information about privacy on social networking sites and none said they did so outside of the provider's website.

When asked about the privacy policy within Facebook, there appeared to be little demand for greater communications efforts on the part of the provider.

Nevertheless, across most groups, there was a consistent request that the “legalese” information on license agreements be edited and formatted in a way that is more readily digestible by users.

Participants did not typically feel that information is kept from them and they did not indicate any particular appetite for the information. However, they did widely (and nearly universally) express that the legal information should be made easier to read in terms of layout and language.

Some offered this is not a situation that is unique for social networking websites, but would also apply to software providers and all sorts of others who use an online agreement.

Among the older groups there was a general feeling that privacy policies should be easier to read for the mere fact that younger generations are even more likely not to read a lengthy privacy policy and to just click without thinking.

By the end of the discussion, after going into detail about some of the specifics on sharing of information by or on social networking sites, most respondents remained unconcerned about any risks posed to their own privacy.

Participants did tend to recommend that social network providers be as clear and upfront as possible with users about what information will be used by whom and how it will be used. The general view was that given a greater degree of education on these issues, although some felt they might slightly alter their behaviour, they tended to say they would remain users. Thus, they felt that it was more respectful for the provider to make the improved effort in this regard.