Globalization of Personal Data Project – International Survey

Findings from the Pre-Survey Focus Groups

Submitted to:
Professor Elia Zurek
Department of Sociology
Queen's University

EKOS

May 2004

Table of Contents

1.0 Introduction

EKOS Research Associates was hired by Queen's University to conduct a series of focus groups in support of the Social Sciences and Humanities Research Council-funded Globalization of Personal Data (GPD) Project.

The GPD Project is an 11-country study of privacy attitudes, involving both quantitative and qualitative research.

The first phase of the project involved a series of preliminary focus groups in advance of commencing the quantitative phase. The main objectives of the pre-focus groups were to provide the research team with qualitative findings in relation to understanding how individuals view the study's areas of research. The findings from this qualitative phase were designed to help shed light on the issues and how they are perceived, with a view to helping frame the questions for the actual survey.

Working with Queen's University, EKOS designed the moderator's guide to address a range of study issues. The moderator's guide encompassed both common and specific issues. Common issues were posed to all participant types, while the specific issues were tailored to the different types (e.g., questions for workers). Where time permitted, some of the specific questions were asked to other groups where relevant (e.g., all travellers are also citizens). All research material was reviewed by the Ethics Review Board at Queen's University prior to conducting the focus groups.

It should be borne in mind when reading this report that these findings are drawn exclusively from qualitative research. While every effort is made to balance various demographic characteristics when recruiting participants, these groups (and therefore the findings drawn from them) may not be said to be representative of the larger population as a whole.

2.0 Research Methodology

The research findings are based on the following:

- In total, eight focus groups were conducted during the week of May 3rd, 2004.

- Focus groups were held in both Toronto and Montreal. The Montreal groups were conducted in French, and the Toronto groups in English.

- The groups lasted approximately two hours and were held in dedicated facilities to allow for viewing by clients and audiotaping.

- A total of 10 individuals were recruited for each of the focus groups. In total, the focus groups involved the participation of 59 individuals.

- Focus group participants were divided into four types: workers, travellers, consumers and citizens.

- The location, dates, type of groups and way in which the participant types were defined is summarized in Table 1.

- All participants received a $60.00 cash incentive.

Table 1
Details of the Focus Groups

Location	Group 1	Group 2	Date
Toronto	Workers	Travellers	May 3rd, 2004
Toronto	Citizens	Consumers	May 4th, 2004
Montreal	Workers	Travellers	May 5th, 2004
Montreal	Citizens	Consumers	May 6th, 2004

- Workers
  - Currently have access to the Internet at work
  - Use the Internet for work related activities "daily/almost daily" in a typical month
  - Range of company sizes (small, medium, large)
  - Range of positions (administrative, management, etc.)
- Travellers
  - Travelled by air at least once in the past year for business reasons
  - One third of participants had also travelled by air internationally (including the United States) at least once in the past five years
- Consumers
  - Half of participants to have purchased a product or service over the Internet before
  - Half of participants are primarily responsible for most of their household's shopping needs
- Citizens
  - Range of age groups
  - Range of income levels
  - Range of education levels
  - Range of household types

3.0 Key Findings

The findings point to a number of over-arching themes that were relatively constant across the different types of participants, although some differences did exist. In broad terms, the findings reinforce the fact that Canadians' attitudes in relation to privacy are complex and extremely context driven.

Perceptions and Experiences with Privacy Issues

As a starting point, the focus groups were designed to ask participants a few high-level questions to gauge how privacy issues are viewed with little or no prompting.

First, participants were asked to write down the first thing that came to mind when they heard the words "privacy" and "security". The responses to this line of questioning around top-of-mind imagery reinforced the fact that both privacy and security mean different things to different people. This line of questioning was designed in particular to help frame some of the high level terminology for the quantitative phase.

- In relation to privacy, participants pointed to many different top-of-mind images, ranging from broad concepts such as confidentiality, secrecy and things that are more subtle and personal, to things related to technologies (and the Internet in particular), to laws/legislation, to the increasing lack of privacy today to the importance of maintaining personal privacy (e.g., they value their privacy, a personal right). Illustrating the diversity in responses, one recently married participant pointed to the bathroom as essentially the only place that this individual now had privacy in their home.

- In relation to security, participants also pointed to many different top-of-mind images. Generally speaking, however, many of the images were diverse and covered both security-related issues in the broader privacy/security context, but also security issues in a non-privacy/security context. Some examples of the former included being safe/protected, peace of mind, terrorism, terrorism and security guards/alarm companies. An example of the latter was "money" (i.e., the security that having money could bring to an individual).

Following top-of-mind imagery, participants were probed on the topic of "privacy as a value". While some participants struggled with what constitutes a value in the first place, others were able to give examples such as freedom and democracy. When probed specifically about privacy, participants tended to lean more towards seeing privacy as right than a value. This, in part, reflected the fact that many assumed that even though laws exist (e.g., assuming that privacy is protected/guaranteed under the Charter of

Rights), personal privacy was still something that required active, individual actions in order to protect.

Despite notable differences in the top-of-mind imagery, there was a strong consensus among participants that the level of personal privacy is eroding in society today. Some participants felt that their privacy has been eroded over the past five years. Others commented that there has been little change over the same time frame as they believed that their privacy had already been under threat before that.

In large part, technology and its greater usage on a day-to-day basis, is seen as the largest single cause of declining levels of privacy today. The increasingly widespread availability and usage of the Internet as well as the usage of other communications and information management technology that facilitate the collection, storage and exchange/sale of personal information were most commonly cited as examples of how technology has changed things. At the same time, the growth in telemarketing was also commonly cited as another example of less privacy, although there are differences in how participants saw the issue. While some participants saw telemarketing as an invasion of their privacy, others saw it more as a nuisance factor.

While virtually all participants believed that there is less privacy today, there were differing levels of concern about it. In fact, it was clear that most participants did not think about privacy-related issues on a regular basis and that, to some degree, many participants felt broader culture is increasingly blasé about some aspects of privacy. Only a small number of participants recalled talking about privacy-related issues with friends or family. Some participants pointed to the September 11th terrorist attacks as providing an "excuse" for increased privacy infringements and the growth in "reality" television programs as a symbol of privacy as a commodity. Despite not being a day-to-day issue that is talked about, privacy is more relevant to some participants than others, reflecting differences in experiences and backgrounds. For example, participants who had experienced a "serious" invasion of privacy were more likely to express concern than others. Likewise, participants who had different ethnic backgrounds expressed different reference points (e.g., differences between Eastern Europe and North America).

Personal Experiences and Concerns

Generally speaking, perceptions about privacy were not based on first-hand experiences for most participants. In fact, only a small number of participants indicated that they had encountered a "serious" invasion of their privacy in the true sense of the privacy debate. Some examples included identity and credit theft, and being spied upon through a peephole. Most personal experiences, however, were at the "nuisance" level (e.g., telemarketers, retail requests for postal codes). Not surprisingly, many participants were able to point to examples of how an individual's privacy could be invaded today.

While few participants had ever experienced it, identity theft was the salient concern for most participants (i.e., beyond fraudulent use of credit card, to include multiple aspects). Awareness of identity theft was relatively high, with examples of debit card fraud being relatively well known. Closely related was the concern for some participants about being falsely accused of a crime, based on identity theft or another type of "mistaken identity".

When probed on whether certain groups in society are more susceptible to invasions of privacy than others, participants pointed to what appeared to be contradictory responses. While some participants suggested that wealthy individuals are more susceptible, others suggested that it was lower-income groups. Wealthy individuals were cited as they, by definition, have more purchasing power and would be more likely targeted as potential buyers. Lower-income groups were cited given that they would be more likely to have to give up personal information if they are to collect government benefits. Other examples of groups that were more susceptible to invasions included ethnic groups/visible minorities, seniors, protestors/activists, as well as famous individuals (e.g., actors, politicians, athletes).

Protecting Personal Privacy

Though not always sophisticated or consistent, a large number of participants point to taking actions to protect their privacy. The most common examples involved being proactive by not giving information, whether they are online or being requested for information. As one participant remarked, they are just more willing to say no today than they used to be. Other examples include the use of technologies such as call screening and simply using common sense.

Somewhat interesting was the fact that a small, but not insignificant number of participants had purchased a shredder for their home to ensure that their bills and other types of information are destroyed.

Expectations Regarding Privacy Issues in the Future

Looking forward, most participants expect further erosions in privacy as technology continues to evolve and as the market for personal information continues to grow.

Despite an extremely limited understanding/awareness of the term "biometrics", most participants were able to comprehend what they could involve and widely expected that usage of biometrics will become commonplace.

Examples of the way in which things may not be as private in the future included:

- Consolidation of various personal information into a single "card" (e.g., one master government card to access services, drive, identify oneself, passport);
- Use of computer chip implants to replace plastic cards;

- Use of personal information to segregate/control people (e.g., extension of gated communities);
- Widespread surveillance (e.g., the film "Enemy of the State");
- Information mismanagement;
- Invention of uses for personal information that cannot be conceived of yet (e.g., marketing); and
- Increased development of "protection technology", along with concomitant increase in new ways of countering these.

Privacy Technologies and Legislation

Technology and Its Uses Seen as Value Neutral

For the most part, participants tended to be pragmatic in their assessment of the technologies and practices that could compromise personal privacy. Against a backdrop of the perceived inevitability of greater usage of technology in the future and growing reliance on technologies like the Internet on a day-to-day basis, most participants were largely value neutral. Like other things, participants saw both pros and cons to technology. Key criteria for judging focused on the purpose, disclosure (i.e., are people aware) and the outcome/efficacy.

While technology uses were seen as value neutral, most participants acknowledged that they did not have enough information to know how technology might affect their personal privacy. Consistent with broader trends, most participants cited the fact that they do not give certain information or give false information while online as a way to protect their privacy. Many participants also talked about learning through "trial and error", having experienced something that they did not want to happen again.

Legislation

The knowledge and awareness of privacy rights and avenues of protection is very low. In fact, few of the participants knew much about any of the different privacy laws in place, including the recent full implementation of the Personal Information Protection and Electronic Documents Act earlier this year. Although many participants imagined that such legal and policy frameworks did exist. Some participants expressed little concern about not knowing about the laws in place given the limited perceived likelihood of something affecting them. As one participant remarked, "I guess until something really bad happens, I'm not going to worry about it too much".

Even when told about privacy laws that exist today, there was, at best, mixed confidence that such laws would be effective at protecting their privacy, regardless of whether they dealt with governments or the private sector. In part, this reflected the perception that the monitoring and enforcement of these laws was assumed to be lax. More importantly, participants generally felt that it was not realistic for Canadians to rely solely on governments to protect their personal privacy. Rather, they saw governments as providing a legal framework in which individuals could exercise their privacy rights (e.g., through the courts). On a continuum with state responsibility at one end and individual responsibility at the other end, personal privacy protection tended to be situated mid-way, but leaning to individual responsibility for many participants.

At the same time, there was broad consensus that individuals have the largest role to play in protecting their own privacy, either reflecting the fact that laws will not be effective if individuals do not take steps to protect their privacy, or the fact that they do not trust that the laws will be followed. As one participant remarked, "we can't just rely on government". Some participants held the view that government is at least as likely to infringe on citizen's personal privacy as is it to protect it. This pointed to the need for individuals to be aware of their rights, be vigilant and know where/how to seek redress.

Privacy Issues and Workers

The issue of monitoring employees in the workplace is a key area of interest of the GPD study given its growing prevalence today. Within this context, the focus groups were designed to probe some participants on this particular issue.

In broad terms, most participants strongly tend to lean towards the acceptability of monitoring in the workplace, with employers seen as having a "right" to do things such as monitor productivity, Internet usage and monitor the use of "company" equipment. Similarly, employers were seen as being able to target or exempt individuals or groups of employees from monitoring should a company decide to do so, again reflecting the notion that employees are on company time when they are working. In fact, most participants believed that monitoring is relatively commonplace today.

Acceptance of employer monitoring of employees tended to be contingent upon employees being made aware of practices and the consequences.

While there was a strong lean towards acceptance of monitoring, some participants drew a fine line between certain activities as well as activities in different parts of the workday. For example, monitoring personal phone calls was seen as far less acceptable, particularly if an employee was only doing it infrequently. In other words, a distinction was made between an employee who makes the odd personal phone call and one that regularly does so. Similarly, a distinction was made between the monitoring of Internet usage and what websites individuals may visit and when someone does so. For example, surfing websites for personal use during breaks and lunch hours was not seen in the same way as doing so during work hours.

Privacy Issues and Travellers

The combination of the September 11th terrorist attacks and the growing proliferation of the worldwide "travel" of electronic data has shifted much of the privacy landscape for travellers, particularly those that cross international borders. Within this context, the focus groups were designed to probe some of the issues pertinent to travellers.

As a starting point, most participants tended to believe that individuals who travel a lot face certain privacy issues that non-travellers do not, particularly those who travel internationally. In the post-September 11th environment, the perception of tighter border control was prevalent among most participants. This was closely related to the perception that some groups are more likely to be singled out crossing international borders, including certain visible minorities and ethnic groups. Some participants spoke about an increased reluctance to travel to the United States as a result. Similarly, one individual who travelled internationally frequently spoke about the fact that certain countries look at which other countries an individual has visited (as shown in their passport) to use as further screening in determining the "risk". This individual held the perception that, for example, Egypt would not allow her to enter the country because she has a stamp in her passport showing that she has been to Israel.

In the focus groups, discussion centred around whether the Government of Canada should track the movements of Canadians as the exit or re-enter the country, and the policy of the American government in relation to requiring advance travel information. While many participants were not very aware of what happens today, there was a strong lean towards the acceptability of such practices, reflecting a strong perceived need for strong security measures.

Here, as elsewhere in the focus groups, participants tended to judge the acceptability of personal privacy infringements based mainly on the practical considerations of effectiveness and cost, as opposed to principles.

Privacy Issues and Consumers

The proliferation of customer loyalty programs in recent years is at the centre of much of the privacy debate today. Within this context, the focus groups were designed to probe this subject and broad attitudes.

To begin, almost all participants participate in one program or another, with only a handful saying they did not. Generally speaking, most participants had a relatively good understanding of the purpose of these programs and how they work (i.e., monitoring purchasing habits), although there was less familiarity with what the company can do with the information it collects (e.g., can it be sold to other companies). When probed on why they participate in these types of programs, participants almost universally point to the "free" things or discounts they get in return.

While not all participants believed they always get good value from participating in these programs (e.g., taking so many points to get anything worthwhile), there was general acceptability of them. Acceptability of how these programs collect and use personal information tended to be based on the legitimacy of practices/usages of information and the attractiveness of the rewards.

Reflecting the near universal participation in these types of programs, most participants acknowledged a willingness to "exchange" personal information for things they need (e.g., apartment, air miles, a loan, a job). In large part, this willingness reflected the fact that most participants did not see a company knowing what they are buying as anything to be concerned about, consistent with EKOS' other research showing that individuals make clear distinctions between different types of information in relation to privacy concerns[1].

Participants who had bought products or services over the Internet were also probed on some of their experiences and attitudes. Despite some broad concerns with the safety of the Internet, most of these participants had still gone ahead and bought online, either for reasons of availability or convenience. It was clear, however, that most of these participants did make some sort of distinction between types of online retailers based on some rough form of reputation. When it came to online privacy policies, there was a mixed outlook: some participants read them closely and others pay little attention. Even those participants who read them clearly are not fully convinced that they are adequate measures of privacy protection.

Privacy Issues and Citizens

In recent years, surveillance cameras have become much more commonplace and have become an important part of the privacy debate. Within this context, the focus groups talked about attitudes towards the usage of these cameras.

As might be expected, most participants were easily able to point to examples of how surveillance cameras are being used today, pointing to examples of convenience stores, cameras in the workplace (both surveillance cameras and the tracking of entry/exit into the workplace using pass cards), traffic cameras, cameras in the subway, cameras in banks/ATMs and those in apartment buildings. The usage of these cameras was seen as acceptable and most understood why they are there.

[1] EKOS' studies have shown that privacy concerns tend to divide into "GIN" and "TONIC" – a term coined by an unknown privacy expert. Concerns are lower with "GIN" – general information and numbers (e.g., a person's name, telephone number) and higher for "TONIC" – technical or other necessary information and communications i.e., information that is often required for a certain transaction (e.g., credit card number). For example, concerns are lower if an activity only requires the submission of an email address, while rising if an individual's income is requested.

The discussion then focused specifically on the usage of surveillance cameras in public places similar to how they are used in London, England and Kelowna, British Columbia. Participants were told that there are approximately 150,000 surveillance cameras operating in London, providing surveillance of almost the entire city. When probed on the usage of surveillance cameras in public places to monitor security/criminal activities and safety, the majority of participants saw it as generally acceptable. Only a small minority were opposed to these types of cameras, but were nevertheless very strong in their views. These views were consistent with the fact that most participants felt that the systematic monitoring of home Internet use by police is acceptable, if it is done so to catch pedophiles for example (although less so for terrorists).

Participants in the Montreal focus groups raised the fact that surveillance cameras had been installed in a downtown neighbourhood known for its high crime rate, but were divided in their views. Interestingly, those participants who were opposed to cameras tended to base their objections not on privacy protection or civil liberty arguments, but on the perceived ineffectiveness of the measures at reducing crime. This was illustrated by one participant's view that the dealers would simply move location and that governments should be investing in social programs aimed at preventing crime instead.

While there was no consensus on whether these cameras would be effective at reducing crime, most participants tended to lean towards a positive assessment. Some participants were less convinced on their usage, although opposition tended to be based not on privacy concerns, but on the view that implementing such as system would be extremely expensive and any funding could a larger impact if spent on crime prevention activities. Likewise, the use of "Black box" in cars came up in the Montreal focus groups and was seen as a good idea if they are mandatory for all cars, drivers are aware and are only used to investigate accidents (not speeding)

When probed specifically about the widespread introduction of surveillance cameras in their city (i.e., Toronto or Montreal), some participants were a little less supportive. Again, the issue of cost to build and maintain was a significant concern. Other participants comfortable with the broad concept were not entirely comfortable with the idea of personally being monitored in a public place.

Ranking of Different Types of Privacy

In the final section of the focus groups, participants were asked to complete a handout that was designed to rate four types of privacy both in terms of the level of importance in protecting and the degree to which these types of privacy are under threat today.

The handout is included in the appendix. The four types of privacy were:

- Bodily privacy (e.g., being watched or monitored without your knowledge or permission);

- Communication privacy (e.g., someone listening to your conversations or reading your emails without your knowledge or permission);

- Informational privacy (e.g., controlling what information is collected about you); and

- Territorial privacy (e.g., not being disturbed at home, being able to have times when you are completely alone, away from anyone else).

The findings, summarized in Table 2, show the following[2]:

- There is a great deal of variability in how participants rank what types of information is important to protect, reinforcing the fact that privacy concerns are individual in nature and context driven.

- All four types of privacy were assigned by at least some participants as the most important to maintain for them personally, with informational privacy receiving the largest number of "most important" ratings across both the Toronto and Montreal focus groups and the lowest average rating (2.08). In Toronto, the pattern was less clear with communication privacy receiving the largest number of "most important" ratings and an average rating of 1.97. Informational privacy was more clearly singled out in the Montreal focus groups with an average rating of 2.07.

- In both Toronto and Montreal, territorial privacy received the largest number of "least important" ratings, although the average rating was only slightly higher than the rating for bodily privacy (2.75 vs. 2.53).

- When it came to the second part of the exercise, there was also a certain amount of variability in the perceived threat to their privacy in the same four types, albeit to a lesser extent.

- In both Toronto and Montreal, informational privacy received the largest number of "most under threat" ratings and the lowest average rating (1.53). The average rating between the two centres was almost identical. Likewise, territorial privacy received the largest number of "least under threat" ratings in both centres, although bodily privacy also scored a high number of the same ratings.

[2] In the first part, participants were asked to rank the four types of privacy in terms of how important it is to ensure that their privacy is maintained in these areas from 1 to 4, where 1 is most important and 4 is least important. Participants were then asked to rank the same four types in terms of the degree to which these areas of privacy are under threat for them, personally from 1 to 4, where 1 is most under threat today 4 is least under threat today. Given the nature of qualitative research, these findings should not be interpreted as statistically representative of the Canadian public.

Table 2
Ranking of Different Types of Privacy

	Ranking			
	Bodily	Communication	Informational privacy	Territorial privacy
Toronto				
Total Respondents	30	30	30	30
Level of Importance				
Most Important (1)	7	10	6	7
(2)	5	13	10	2
(3)	10	5	8	7
Least Important (4)	8	2	6	14
Average	2.63	1.97	2.47	2.93
Level of Threat				
Most Under Threat (1)	3	4	20	4
(2)	8	13	5	4
(3)	7	10	4	8
Least Under Threat (4)	7	10	4	8
Average	2.93	2.40	1.53	3.07
Montreal				
Total Respondents	29	29	29	29
Level of Importance				
Most Important (1)	9	7	14	8
(2)	6	13	3	8
(3)	7	5	8	2
Least Important (4)	7	4	4	11
Average	2.41	2.21	2.07	2.55
Level of Threat				
Most Under Threat (1)	7	11	16	8
(2)	3	9	12	4
(3)	12	7	0	6
Least Under Threat (4)	7	2	1	11
Average	2.66	2.00	1.52	2.69
Toronto and Montreal				
Total Respondents	59	59	59	59
Level of Importance				
Most Important (1)	16	17	20	15
(2)	11	26	13	10
(3)	17	10	16	9
Least Important (4)	15	6	10	25
Average	2.53	2.08	2.27	2.75
Level of Threat				
Most Under Threat (1)	10	15	36	12
(2)	11	22	17	8
(3)	19	17	4	14
Least Under Threat (4)	11	22	17	8
Average	2.80	2.20	1.53	2.88

Conclusions

The findings from the focus groups pointed to a number of cross-cutting conclusions. In summary, the main conclusions are as follows:

- Personal privacy is seen as eroding, driven mainly by technological evolution.

- Most participants appear resigned to a future with less privacy.

- Participants tend to pragmatically assess the acceptability of privacy invasions or intrusions based on key criteria (e.g., purpose, effectiveness, cost, disclosure and awareness). Awareness is a particularly important issue given that it is often low.

- Few participants spoke of personal privacy as a value or in philosophical terms (e.g., linked to civil liberties, freedom or democracy). Instead, participants view personal privacy as a "right" that can only be effectively safeguarded by the individual through knowledge, awareness and, ultimately, vigilance and action/redress.

- Governments are seen as providing legislative and other protections (e.g., Privacy Commissioners, Ombudsmen), but are not perceived to be in a position to effectively monitor compliance or enforce (i.e., there are simply too many transactions/instances, and not enough resources).

- At the same time, the credibility of government as privacy guardian is diminished by view of government as a potentially prime invader of personal privacy.

- Despite primacy accorded individual action, most acknowledge that they have adopted a laissez-faire attitude to their personal privacy, relying on government and the good will of the organizations with whom they do business.

- The proliferation of technology and instances where personal information or other forms of personal privacy are at stake have become too numerous and complex for the average person to be vigilant about.

- Ambivalence and stoicism is reinforced by the fact that most have yet to suffer serious personal consequences of a privacy invasion (e.g., banks absolve clients of liability for fraudulent credit card use).

4.0 Implications for the Quantitative Phase

The findings from the focus groups point to a number of key issues to take into account in the quantitative phase of the study.

- Privacy is not something that most individuals will think about on a day-to-day basis, suggesting the need to design a number of introductory questions to set the context. This is likely to be even more important in countries where privacy rights and laws are not as well as established compared to the westernized countries such as Canada, the United States, and Britain in the study.

- The findings reinforce the complexity and context driven nature of privacy concerns and the fact that privacy (and security) will mean different things to different individuals within the same country, let alone across countries. This reinforces the value in having “vignettes” to describe some examples to gauge attitudes on a comparable basis across countries.

- It is also clear that there is a continuum on the privacy protection front, where the perceived roles of the state and the individuals will differ. For example, respondents may have perceptions about the role of the state when asked broadly, but would make notable distinctions in relation to health information and purchasing habits, for example.

- In addition to the basic demographics, there may be value in considering the addition of various “background” types of questions important from an analytical point of view. Some examples include having experienced invasions of privacy, confidence in governments to follow laws, sense of individual responsibilities in protecting their own privacy, and proxies for specific actions that individuals have taken to protect their privacy (e.g., withholding information).

Appendix A: Moderator's Guide

Globalization of Personal Data Project – International Survey

Moderator's Guide

1. Introduction (5 minutes)

- Moderator explains the purpose of the research and who is the client.

- Mention that the discussion is being audiotaped as the moderator cannot take good notes during the focus group.

- Mention that participants are being observed by members of the research team.

- Confidentiality: Explain that the findings from the focus groups are kept confidential. No full names will be associated with any information provided in this discussion group. The report will simply describe patterns of opinions over the series of focus groups.

- Explanation of format and "ground rules": there are no wrong answers/no right answers, okay to disagree, individuals are asked to speak one at a time.

- Moderator's role: raise issues for discussion, watch for time and make sure that everyone gets a chance to speak.

- Ask participants if they have any questions before beginning.

- Participant introductions: ask participants to introduce themselves by their first name only and to say a little bit about their background (e.g., occupation/status).

2. Perceptions and Experiences with Privacy Issues (35 minutes)

- When you hear the word "privacy", what is the first thing that comes to mind?

  [Moderator instructs participants to write down the first thing that comes to mind.]

- And when you hear the word "security", what is the first thing that comes to mind?

  [Moderator instructs participants to write down the first thing that comes to mind.]

- Respondents are then asked to read what they wrote down about "privacy" and "security".

- People often talk about privacy as a value. What is a value [PROMPT: freedom, equality are often cited as values]? What about privacy as a value?

- In our surveys, we often ask people about privacy, and whether or not they feel that they have less privacy in their daily life than they did five years ago. How would you answer this question?
  - Can you tell us why you feel that way?
  - In what areas do you have less privacy?

- How concerned are you about your privacy today? ·
  - What kinds of things do you do to protect your privacy?
  - Where do you generally get your information about privacy issues?
  - Have you ever discussed these issues with family, friends?

- How have your views changed in the past five years? In what ways?
  - What prompted these changes? Is anything different since September 11th?

- Has anything you have seen in the media (TV, radio programming, newspaper, magazines, online information or advertising) prompted these changes? How so?

- Have you ever experienced a serious invasion of privacy?
  - What kind of invasion of privacy was it?

- Can you give me some examples of privacy invasions?
  - Invasions in your day-to-day lives?
  - Invasions by government?
  - Invasions by companies?
  - Invasions in the workplace?

- What are some other ways that your privacy could be compromised?
  - [Prompt if necessary: identity theft, credit information, credit card, financial information, surveillance cameras, tracking of purchases].

- Are some groups in society more susceptible to invasions of privacy than others? Which groups? [PROMPT: Low-income, visible minorities, ethnic groups] Why do you say that?

3. Expectations Regarding Privacy Issues in the Future (15 minutes)

- How likely is it that you will actually experience a serious invasion of your personal privacy over the next five years? What type of invasion could you see happening?

- Compared to today, do you think that the threat of an invasion of your personal privacy will be greater or less in ten years from now? Why do you say that?

- What do you think may not be as private in the future?

- If I asked you to pick one thing, what would you say is the biggest threat to your privacy in the future?

- How do you think technology will affect your personal privacy in the future?

4. Awareness of and Attitudes towards Privacy Technologies and Legislation (30 minutes)

Technologies

- How much do you rely on electronic or computer-based technology in your daily life, either at home or at work?
  - What types of technology do you use?
- How confident would you say you have enough information to know how technology might affect your personal privacy? What about the Internet?
- How could the Internet affect your privacy? And what about email?
- Are you aware of things that you could do to protect your privacy while on the Internet?
  - Have you ever done anything to protect your privacy while on the Internet?
- Have there been any changes with respect to the use of these technologies by companies/governments in the past few years when it comes to your privacy?
  - In what way have things changed?
  - What do you think prompted this change?

Legislation

- What things exist to protect your privacy today? What laws exist?
- Are you aware that there are federal privacy laws that place strict restrictions on how federal government departments use personal information, including restrictions on the sharing of personal information?
  - To what extent do you believe these laws are effective at protecting your privacy?
- What about laws that place restrictions on how companies use personal information, including restrictions on the sharing of personal information?
  - To what extent do you believe these laws are effective at protecting your privacy?

- [As some of you mentioned] some measures aimed at increasing security are, at times at the expense of privacy. Do you think this is currently the case?
  - Specifically, what security measures compromise privacy?
  - On balance, do you feel these measures aimed at increasing security are justified?
  - What about in the future? Do you expect the emphasis will be more on "security" or "personal privacy"?

5. Privacy Issues Specific to Workers (25 minutes)

- To what extent do you think companies keep track of the activities of employees while they are in the workplace?
  - Are they tracking how much time employees spend online, maintaining a list of websites employees visit and information entered? Emails sent or received?
  - Should they be allowed to monitor these types of activities of their employees? What types of activities? Why? Why not?
  - What is and isn't personal information in the workplace?
- Do you know if your employer uses any methods to track the actions of their employees? How do you feel about this?
- Do you believe businesses are required to inform employees and prospective employees of different methods they may use to monitor workplace activities?
- Should employers be able to monitor all their employees equally or should they be able to target or exempt individuals or groups of employees from monitoring?

6. Privacy Issues Specific to Travellers (25 minutes)

- Do people who travel a lot face any privacy-issues that non-travellers do not? What about those that travel regularly between other countries? What types of things are different?

- To what extent should the Government of Canada track the movements of Canadians as they exit or re-enter Canada? Should information collected be shared with other governments or international agencies? Why do you say that?

- After September 11th, the United States required advance information on air travellers destined for the United States. As such, the federal government had to comply and ensure that this information is transmitted ahead of time.
  - Were you aware of this requirement? What, if any concerns, do you have with this?
  - What do you think of the fact that Canada had to comply (i.e., they did not have a choice)?

7. Privacy Issues Specific to Consumers (25 minutes)

- How many of you have ever participated in a customer loyalty program such as Airmiles?
  - What is the purpose of these programs?
  - Why do you participate?
  - What type of personal information do they collect? What do they do with this personal information?
  - Can they sell this personal information to other companies? Under what circumstances can they? [FOR THOSE IN LOYALTY PROGRAMS] Have you given consent?

- As some of you may know, when individuals take part in a loyalty program such as Airmiles, each time they use their card to collect points, the Airmiles company keeps track of the items they have purchased. These companies can then sell this "purchasing behaviour" information to other companies participating in the Airmiles loyalty program.
  - What do you think of a company being able to track purchases?
  - What do you think of them being able to transmit that information to other companies?
  - What kinds of things is it ok for companies to monitor?

- Have any of you ever made a purchase over the Internet? Why/why not?
  - What prompted you to make your first purchase over the Internet?
  - Did you think it would be safe?
- What about privacy policies on websites and e-commerce websites in particular?
  - What do you think of these policies?
  - Who actually reads them?
  - Are they adequate measures of privacy protection? Are they all equal, or does your view about the privacy policies depend on the company? Why?

8. Privacy Issues Specific to Citizens (25 minutes)

- Let's turn to the issue of surveillance cameras. How are surveillance cameras being used in your community? How are they being used elsewhere in the country?
  - Where are they located?
  - What are they used for?
  - Who operates them?
  - What purpose do they serve?
- In London England, and in some Canadian communities, such as Kelowna B.C., police are using surveillance cameras to monitor public places in order to deter crime and assist in the prosecution of offenders? In fact, there are roughly 150,000 surveillance cameras operating in London.
  - What do you think of surveillance cameras in public places? What are the pros? What are the cons?
  - Do you think this is an effective way to reduce crime?
  - Are their other more effective ways?
- What would you think if a large city like Toronto or Montreal was to follow the lead of a London, England and introduce surveillance cameras all across the city?
  - Good idea? Bad idea?

- Would you have any concerns? What?
- How comfortable are you with the idea of being monitored by a police surveillance camera as you walk down a street or go to a park?

9. Concluding Questions (10 minutes)

- Have participants answer the handout.
- Is there anything else you would like to add before we end the discussion?

THANK YOU FOR YOUR PARTICIPATION!

ATTITUDES ON PRIVACY

Some privacy experts talk about four different types of privacy: bodily privacy, communication privacy, informational privacy, and territorial privacy.

How would you RANK these different types of privacy in terms of how important it is for you to ensure that your privacy is maintained in these four areas? [Please rank the four types listed below with a 1 to 4, where 1 is most important and 4 is least important].

Bodily privacy (e.g., being watched or monitored without your knowledge or permission) ______

Communication privacy (e.g., someone listening to your conversations or reading your emails without your knowledge or permission) ______

Informational privacy (e.g., controlling what information is collected about you). ______

Territorial privacy (e.g., not being disturbed at home, being able to have times when you are completely alone, away from anyone else) ______

And how would you rank the same four types in terms of the degree to which these areas of privacy are under threat for you, personally? [Please rank the four types listed below with a 1 to 4, where 1 is most under threat today 4 is least under threat today].

Bodily privacy (e.g., being watched or monitored without your knowledge or permission) ______

Communication privacy (e.g., someone listening to your conversations or reading your emails without your knowledge or permission) ______

Informational privacy (e.g., controlling what information is collected about you). ______

Territorial privacy (e.g., not being disturbed at home, being able to have times when you are completely alone, away from anyone else) ______