# EXPLORING THE PRIVACY CONCERNS AND PRIORITIES OF CANADIANS

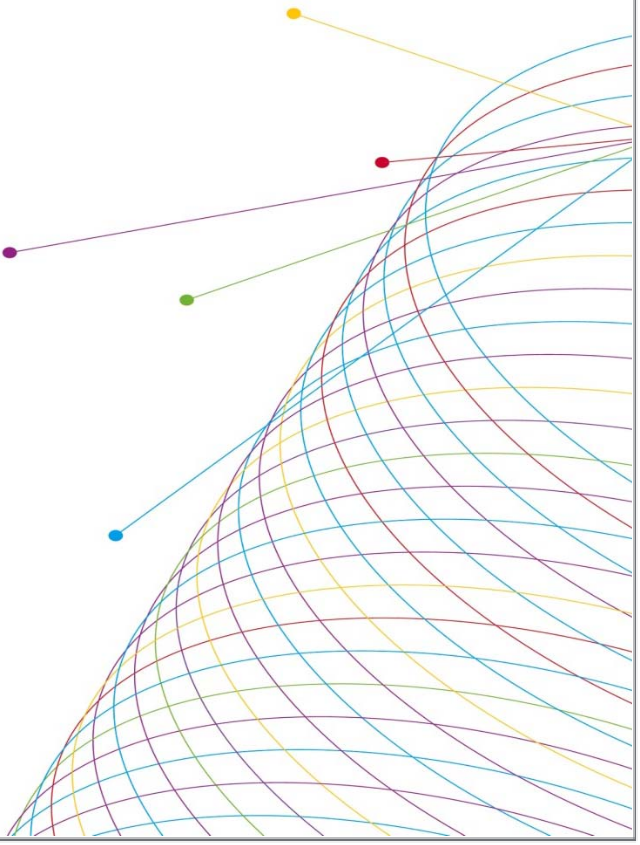
## FINAL RESEARCH REPORT

## PREPARED FOR:
## THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

## FEBRUARY 2015

Contact Information: publications@priv.gc.ca

*Ce rapport est aussi disponible en français*



## PROPRIETARY WARNING

Any material or information provided by the Office of the Privacy Commissioner of Canada and all data collected by Nielsen will be treated as confidential by Nielsen and will be stored securely while on Nielsen's premise (adhering to industry standards and applicable laws).

**OTTAWA**
1800-160 Elgin St.
Ottawa, Ontario, Canada
K2P 2P7

Tel: (613) 230-2200
Fax: (613) 230-3793

**TORONTO**
405-2345 Yonge St.
Toronto, Ontario, Canada
M4P 2E5

Tel: (416) 962-2013
Fax: (416) 962-0505

**MONTRÉAL**
400-1080 Beaver Hall Hill
Montréal, Québec, Canada
H2Z 1S8

Tel: (514) 288-0037
Fax: (514) 288-0138

## Table of Contents

# EXECUTIVE SUMMARY

## Background and Methodology

Nielsen Consumer Insights (Nielsen) is pleased to present this report to the Office of the Privacy Commissioner of Canada (OPC) based on qualitative research to explore Canadians' immediate and emerging privacy concerns.

The OPC is currently conducting a priority-setting exercise. To help inform this exercise, the Office is exploring Canadians' privacy concerns and priorities in more depth. The research is intended to build on quantitative public opinion research conducted on behalf of the Office every two years with Canadians. The findings will be used to help guide the Office's forward-thinking work in order to ensure that it is, and remains, ahead of the curve on emerging areas that are likely to be or become of importance to Canadians. They will also be used to inform the Office's outreach and public education work.

The findings in this report are based on eight focus groups conducted in Vancouver (2), Montreal (2), Halifax (2), and Toronto (2) between December 3rd and 10th, 2014. In each city, one group was conducted with the general population and a second conducted with "engaged Canadians" (defined as those who self-identified as following news and public policy somewhat or very closely). All sessions were standard groups, two hours in length, with up to ten (10) participants each. Sessions began at 5:30pm and 7:30pm each evening, and participants were given an honorarium of $75 in appreciation for their time.

The following table outlines the groups in terms of date, location, language, and target audience:

| City | Date | Language | General Population | Engaged Canadians |
|---|---|---|---|---|
| Vancouver, BC | December 3rd | English | 1 | 1 |
| Montreal, QC | December 8th | French | 1 | 1 |
| Halifax, NS | December 9th | English | 1 | 1 |
| Toronto, ON | December 10th | English | 1 | 1 |
| **Total** | --- | --- | **4** | **4** |

The focus groups began with a general discussion about participants' knowledge and concerns related to privacy followed by an exploration of seven specific potential privacy priorities through a written exercise and discussion about concerns related to each priority.

Appended to this report are the recruitment screener, discussion guide, and focus group handouts used.

*NOTE: For the purposes of this report, it is important to note that focus group research is a form of scientific, social, policy and public opinion research. As structured, restricted, group interviews that proceed according to a careful research design and attention to the principles of group dynamics, focus groups should be distinguished from* *"discussion groups", "problem-solving groups", "buzz groups", or "brainstorming groups". They are not designed to help a group reach a consensus or to make decisions, but rather to elicit the full range of ideas, attitudes, experiences and opinions of a selected sample of participants on a defined topic. Because of the nature of focus of focus groups (e.g., the impact of group dynamics, a lack of standardization in how questions are asked, etc.), however, findings cannot be assumed to be representative of the larger population.*

## Key Findings

The concept of privacy is different for each person but generally participants understand it to mean that they control how and when personal information is used and shared. Many participants were quick to note their sense of loss of privacy in our increasingly digitized world. Most participants have come to expect that their personal information is being monitored, stored, shared, etc., although they are not entirely comfortable with the idea. For some, there is a sense that "I have nothing to hide, so I have nothing to fear", and many feel they do not have much control or influence over determining what is, or is not, acceptable with respect to personal information that is collected by others.

Privacy on the Internet is a primary concern for most participants. A number of participants try to restrict their online behaviour or limit their information sharing to protect their privacy, but even those very concerned about privacy do still use the Internet for some services. Some are comfortable giving up their privacy if there is a perceived benefit, such as providing demographic information in exchange for a reward (e.x., discount, coupon, reward points, etc.) from an organization. Others are comfortable with government surveillance if the information is used for national security, crime prevention or fraud detection (e.x., flagging unpaid parking tickets, system fraud such as Employment Insurance, etc.). Participants are most concerned about financial and medical information, but concern is heightened when participants have personally experienced a privacy breach, such as identity theft, credit card fraud, or a damaged reputation.

Participants' opinions about responsibility for protecting information varies slightly depending on the privacy topic, but generally most start from the premise that the individual is responsible for sharing the information they feel comfortable sharing. They feel organizations have an ethical responsibility to protect the personal information they collect. With respect to the government, participants expect the government to establish, monitor and enforce privacy laws. Additionally, they look to the government to educate Canadians about privacy issues, provide guidance on how best to protect their personal information, and be open and transparent about their own use of citizens' personal information.

## PROTECTING CANADIANS IN A BORDERLESS WORLD

This topic explores the fact that in a globally networked and integrated economy personal information can move with ease around the world. For example, businesses may transfer personal information to other countries for processing or storage, and individuals are also increasingly sharing their personal information abroad through the increased use of cloud services or online shopping. Participants are consistently the most concerned with this topic, particularly given their assumption that privacy laws in other countries may not be as stringent as in Canada. Participants feel a greater sense of powerlessness and loss of control of their information when they imagine it being stored (and thus accessible) in other parts of the world. While most are dubious about the handling and storage of information within Canada, they generally expect that there are even fewer safeguards in place in other parts of the world, particularly outside of North America. Main concerns centre around organized crime and the black market for identity theft and fraud.

## REPUTATION & PRIVACY

This topic focuses on personal reputation management in a digital world. Awareness and understanding of the potential negatives associated with this topic is high. This is why a number of participants indicated that they restrict their online behaviour and activities (to varying degrees). Concerns about cyber bullying or the potential for the misinterpretation of information that could affect employment or other services are often cited as potential negatives associated with having an online reputation. Those less concerned with this topic tend to feel that they sufficiently restrict the personal information they share online, they trust their friends and acquaintances to not use the shared information maliciously and feel that they have nothing to hide.

## STRENGTHENING ACCOUNTABILITY AND PRIVACY SAFEGUARDS

This topic explored the importance of responsibility and accountability with respect to the handling of personal information—for both individuals and organizations. While most are concerned about the protection of their privacy, there is an assumption that companies and governments are not doing all they can to protect the privacy of their customers' information. Individuals with higher levels of concern take it upon themselves to curtail their use of online services. Others cite concerns with certain services, but note they continue to use them for the convenience and benefits. The overwhelming majority of participants, however, say it would be helpful to educate Canadians by providing them with some best practices for privacy protection.

## THE BODY AS INFORMATION

This topic looked at information extracted from the body and stored by various organizations, including medical and non-medical. The issue of digitized, highly personal information about the body being collected is of varying concern to participants. Participants feel the potential risk of security breaches and misinterpretation of information is most concerning, although there is a sense that certain (unique) identifiers, such as thumbprints and heart rates, do increase security protection. Participants generally feel the technology and associated privacy risks related to this topic are still in early stages and that it will become a more important priority in the not too distant future.

## GOVERNMENT SURVEILLANCE

This topic focuses on government surveillance and the impact that advances in technology are having on the collection of personal information for this purpose. Participants tend to be somewhat less concerned about surveillance when it relates to the government's role in protecting national security and preventing crime because they feel there are benefits for society as a whole. However, some feel that there is a fine line between security and a threat to democracy, and some cited concerns about a 'Big Brother' approach. Most expect that they are being watched and recorded pretty much everywhere now, and have varying levels of comfort with the idea. There is heightened concern around use and potential misinterpretation of the data collected. There is also a sense that surveillance activities could lead to an individual being labeled or profiled in a way that negatively impacts their life. Building on this sentiment, most believe the government should be open and transparent in informing Canadians about what is being monitored, by whom and for what purpose.

## ECONOMICS OF PERSONAL INFORMATION

This topic explored the increasing trend towards providing personal information to private-sector organizations in exchange for benefits or access to services. Most participants are aware of the privacy risks associated with using online services. They are aware that companies use their personal information to send them tailored ads or market to their interests and this is mostly viewed as a nuisance. For those concerned with this topic, the most important threat (and what tends to curb most of their online behaviour) is identity theft. Participants are worried about the potential long-term financial implications of this outcome. That said, a number of participants indicated they are willing to exchange personal information for what they feel is a favourable benefit or reward.

## GOVERNMENT INFORMATION SHARING

This privacy topic relates to sharing of personal information among government departments. Concern about privacy protection in this instance is mixed. Those with higher levels of concern worry about the 'Big Brother' aspect of government access and control over personal information. There is also a sense that government does not adequately protect the personal information it has (i.e., many speak of recent breaches). Those with lower levels of concern like the idea of having improved government services if departments and agencies were sharing information. There is a certain amount of trust in the Canadian government to store and share the appropriate information, with the right agency/department, at the right time.

Of the seven privacy issues summarized above, the issue of most concern to participants was Protecting Canadians in a Borderless World, followed by Reputation and Privacy and Strengthening Accountability and Privacy Safeguards. However, participants indicated a relatively high level of concern for all issues discussed. When probed about who they see as being responsible for protecting privacy, in many cases participants felt that individuals play a key role in adapting their own behaviour to avoid negative consequences of releasing private information, while, government has the responsibility of setting laws and regulations that organizations will abide by.

**More Information:**

Supplier Name: Nielsen Consumer Insights
Contract Number: 2R008-14-0173
Award Date: November 3, 2014
Contract Amount: $45,092.65 (including HST)
OPC contact: publications@priv.gc.ca

# DETAILED FINDINGS

This report is divided into three sections. The first section discusses participants' views of privacy and their top-of-mind concerns. This is followed by an in-depth exploration of specific privacy priorities and participants' concerns with each. The third and final section looks at what actions the federal government could take to alleviate some of their concerns.

## A. General Knowledge and Concern About Privacy

Each focus group began with a discussion about personal privacy and the protection of personal information. Participants were asked to share what privacy means to them and what concerns they have about the protection of their privacy.

### PRIVACY IN GENERAL

Most participants have the sense that it is very difficult to protect one's privacy today, particularly in the digital world. Most have come to expect that their personal information is being monitored, and have varying levels of comfort with this reality. Conversations quickly turned to concerns about privacy protection online; privacy on the Internet is a primary concern. Many participants used terms such as "prudent", "vigilant" and "careful" when discussing their online activity and behaviour.

Those who have concerns about the protection of their personal privacy feel the need to censor themselves, which they note to be a nuisance. Participants expressed feeling that they have less control over what personal information is shared and accessed. They have concerns over how their personal information is being used and are particularly concerned about criminals using it to steal their identity or steal money from them. For others who are less concerned, there is a sense that "I have nothing to hide, so I have nothing to fear." They feel that they don't have much control or influence over determining what, and how much, personal information is required or collected by organizations and government.

In many groups, participants indicated that they think organizations should have to seek consent to collect, store and share personal information, and this would go a long way in alleviating their concerns.

Older participants have the sense that protection of privacy is particularly worrisome for the younger generations who are growing up in the digital world. In reality, younger participants have similar concerns with respect to the protection of privacy as other participants; while a number of online activities were cited by the younger participants, they feel aware of the risks involved and will share their personal information based on their comfort level.

## ADAPTING BEHAVIOUR GIVEN PRIVACY CONCERNS

A number of participants try to restrict their online information sharing and activities to protect their privacy (e.x., avoid social media, online purchases, divulging their personal information) but even those very concerned about privacy do still use the Internet for some services. Those active online are using the Internet for searches, online banking, making purchases, booking travel, reviewing restaurants and hotels, etc., but social media is often cited as where some draw the line because they feel that using this medium unduly risks exposing their personal information.

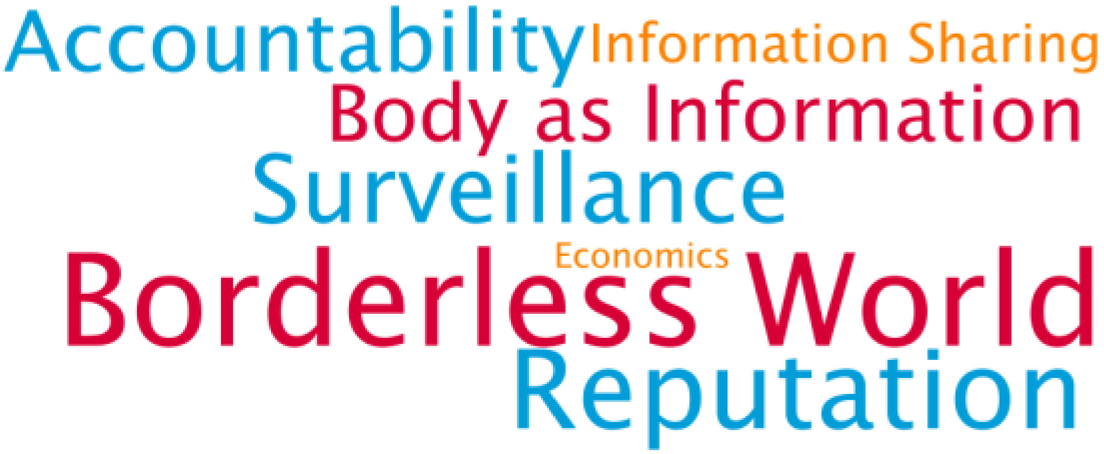
Some of the things participants currently do to mitigate their concern and protect their personal information include the following:

- Limit exposure/what they do on the Internet (i.e., limit online purchases, use of social media, etc.);
- Ensure their computers have anti-virus software, delete cookies, etc.;
- Keep passwords protected and change passwords frequently;
- Only frequent trusted websites—some look for the secure padlock symbol;
- Set up separate email accounts for purchases, coupons, discounts, etc.;
- Use Internet payment companies for online purchases;
- Use multiple credit cards or a dedicated credit card for online purchases; or
- Log off of websites as soon as they are done to ensure nothing is left open and/or accessible.

## B. Exploration of Proposed Privacy Priorities

The majority of each group was spent exploring specific privacy topics. Participants were given seven handouts summarizing different privacy topics. All but one handout included an accompanying visual to help participants digest the concept and spark conversation.

Participants were asked to rate their level of concern for each topic on a 7-point scale (7 being *extremely concerned;* 1 being *not at all concerned*) and, once all topics had been discussed, to rank their top three privacy concerns. The overall findings of these exercises are presented in the word cloud that follows. The larger font in the word cloud below signifies higher levels of concern. As the word cloud illustrates, participants appeared to be most concerned about *Protecting Canadians in a BORDERLESS WORLD*. The topics that were the next tier in terms of levels of concern include: *REPUTATION and Privacy; Strengthening ACCOUNTABILITY & Privacy Safeguards; the BODY AS INFORMATION; and, Government SURVEILLANCE*. The two topics that were met with lower levels of concern were *Government INFORMATION SHARING and ECONOMICS of Personal Information*.



The remainder of this section details the findings for each privacy topic. The topics are discussed in order of the concern attributed to them by participants. For each topic we present the synopsis participants were provided, a summary of the discussion, the level of concern, the perceived benefits and concerns, as well as some of the specific comments heard in the focus groups.

## PROTECTING CANADIANS IN A BORDERLESS WORLD

***Synopsis***

In a globally networked and integrated economy, personal information and data can move quickly and effortlessly around the globe:

- Individuals use cloud services for photo sharing, social networking or email, and shop online with businesses based in other countries.
- Businesses may transfer the personal information they collect to organizations in other countries for processing or storage.
- Governments share personal information with other countries for law enforcement and security purposes.

When data moves around the world, it can end up in countries that have weak privacy protections or none at all.

When data is collected by companies operating in many countries, data breaches or changes to terms and conditions or policies can impact individuals around the globe.

Overall, this was the topic that was the most troubling for participants. Most are not comfortable with personal information being shared and stored in other countries; in fact, many participants were unaware that this occurs. Participants feel a sense of powerlessness and loss of control of their information when they imagine it being stored (and thus accessible) in other parts of the world. Concerns were expressed about the possibility that businesses and governments in other countries may not have strict enough laws or enforcement for privacy, with some citing worries about organized crime and the black market seeking out private information (particularly financial) for identity theft or fraud. While many participants are also dubious about how information is secured and protected within Canada (many have heard of breaches by the Canadian government in the past) they still feel that the rules and regulations within Canada—and North America in general—are more strict than in other parts of the world and should be applied to any information collected about Canadians.

With respect to privacy protection, the majority of participants believe responsibility for protecting personal information should be shared. For the example of Internet cloud services, participants believe it is up to the individual to decide whether they want to do business with these organizations or use these services, so they feel it is important for individuals to use good judgment when sharing their personal information. For the example of businesses transferring information to organizations in other countries, most believe there is a shared responsibility between businesses and government to protect that personal information (e.x., create regulations or laws that are punishable if breached). In the instance where governments share information for law enforcement and security purposes, participants feel it is the government's responsibility, though some are concerned that sharing this information could mistakenly create border issues or impact travel to other countries; however as we will see later, when government use of personal information is for the purpose of protecting Canadians (i.e. national security, crime, etc.) most tend to be more comfortable with this use.

| | | |
|---|---|---|
| Level of Concern | Extremely concerned (7) | 20 of 63 |
| **Mean 5.4** | **Concerned (5-6)** | **26 of 63** |
| | Neither (4) | 12 of 63 |
| | Not concerned (2-3) | 4 of 63 |
| | Not at all concerned (1) | 1 of 63 |
| Benefits | ✓ None | |
| Concerns | ✗ Identity theft/fraud<br>✗ Questionable legislation and protection laws in other countries; organized crime/black market<br>✗ Potential loss of freedoms/liberties in terms of government surveillance<br>✗ Distance/sense of helplessness/lack of control<br>✗ Uncertainty about the security of cloud services (particularly when data is stored in other countries) and risk of personal information being compromised | |
| In their own words… | ***"I worry because other countries don't have the same legislation and protection laws. There is organized crime and a black market for my credit card information."***<br>***"Government sharing for law enforcement might translate into loss of personal freedom. I don't want to travel and be arrested at the border."***<br>***"I'm bothered by what information [companies] have…I'm worried about how it will be transferred and why it would be transferred."*** | |

## REPUATION & PRIVACY

***Synopsis***

Our reputations reflect how others perceive us—and they can affect us both personally and professionally. The Internet has had a profound impact on personal reputation management. On the Internet, we shape our reputation by posting social media profiles, photos, online comments, etc. Our digital trails can also paint a picture of us—the sites we visit, where we shop, and our movements via the GPS on our phones. But others can shape our reputation as well by posting information about us. Personal information can be easily posted, duplicated and shared on the web, but it can also be challenging to remove, correct or control.

A number of participants think carefully about what information they share online and restrict their online activities to ensure they have as much control over their reputations as possible. Some may limit their footprint by only sharing information online with friends, while some will go as far as keeping all information to themselves, such as using "incognito mode" when doing Internet searches, using advertisement blockers to limit the collection of their personal information for targeted advertising campaigns, or opting out of social media. Overall, most realize that once the information is out there it is difficult to control or remove.

Awareness and understanding of the potential negatives is high. Many cite instances of cyber-bullying, -harassment or -defamation that have been reported in the media and express concern about how these negative behaviours may affect youth. Many also note the workplace implications of the increasing practice of organizations reviewing an employee's (or potential employee's) Internet presence and feel that employers should not be able to judge them according to their personal lives. Those less concerned with this topic tend to feel that they trust their friends and acquaintances to not use the shared information maliciously. Others feel that they have nothing to hide and are, therefore, not concerned about negative consequences of having an online reputation. Additionally, some are less concerned since they feel that the actions they are taking to limit their digital footprints protect them from this issue entirely. Managing privacy settings was one example of this type of action, although some also indicated frustration with using these settings given that they can be complicated and frequently changing.

In terms of responsibility, most feel it is up to the individual to protect their privacy (hence why they limit their online activities). There is a sense that one cannot count on businesses to protect their privacy, although a few felt businesses (i.e., social media sites) should take some responsibility to identify and address instances where personal information is being used in a way that negatively affects others.

| | | |
|---|---|---|
| Level of Concern<br>**Mean 5.0** | Extremely concerned (7) | 11 of 63 |
| | **Concerned (5-6)** | **31 of 63** |
| | Neither (4) | 11 of 63 |
| | Not concerned (2-3) | 8 of 63 |
| | Not at all concerned (1) | 2 of 63 |
| Benefits | ✓ None | |
| Concerns | ✗ Online bullying, embarrassment<br>✗ A person's reputation can be compromised by others<br>✗ Someone's online personal information being used by others to make decisions about them—personally or professionally<br>✗ Surveillance<br>✗ Difficult to undo the damage (can never remove/erase it) | |
| In their own words… | ***"My reputation can be tarnished by others; I have no control."***<br>***"You can't control what your friends do. Information can be used to discredit you. It's about your reputation."***<br>***"My concern is being followed. Your cell phone has GPS. Your employer can be looking at your info. You're being followed and monitored."***<br>***"I'm really bothered by it because it's so easy to cyber bully and post information about people and say things that are harmful and hurtful."***<br>***"You cannot remove it, ever. So if something goes up negatively, it never goes away."*** | |

## STRENGTHENING ACCOUNTABILITY & PRIVACY SAFEGUARDS

***Synopsis***

Organizations have a responsibility to protect the personal information in their care. As more and more information is collected, processed and stored electronically, organizations must continually update their privacy practices and security measures to ensure that personal information will not be stolen, misused, leaked or lost. Organizations also need to clearly and proactively explain what personal information is collected, how it will be used and if it will be shared with any other organizations.

Individuals can take steps to improve their own privacy management practices by adopting good security practices (e.x., passwords), reading privacy policies and user agreements, adjusting privacy settings, and thinking carefully about the information they share or post about themselves and others.

Most are concerned about the protection of their privacy and there is an assumption that companies are not doing all they can to protect the privacy of their customers/users information; however, they feel that they have to trust someone. Those with higher levels of concern curtail their use of online services. Others continue to use online services despite their privacy concerns, citing the convenience and benefits. Most do online banking and there is a sense that banks are among the most trusted organizations; participants cite examples of good interactions with banks and note that their comfort level stems from rarely or never having had any negative issues related to their personal information being compromised by banking institutions. Participants expressed similar sentiments about some larger organizations noting that they feel they can trust them with their personal information because they have a history of good and safe transactions. In the end, however, participants feel that a security breach is inevitable with advancing technology and capabilities of hackers who want to exploit this information.

The overwhelming majority of participants do not read the user agreements and policies provided to them when signing up for services; they are seen as complicated, legalistic and difficult to understand. At best, some participants noted that they see user agreements as a formality that needs to be completed in order to access the services they want. In many cases, participants would feel safer if organizations and government were more upfront with them about how their personal information is being used—rather than having to ask. They also emphasized their desire to have control over what personal information organizations collect and what they can do with it.

In terms of responsibility, most believe responsibility is shared between individuals and businesses. “It’s good business for them to have more robust, secure systems.” However, there is some uncertainty that businesses are doing everything they can do to protect privacy. Participants believe it is up to the individual to decide with whom they want to share their personal information. Many participants would appreciate a reminder about adopting good security practices (e.x., passwords, reading policies, adjusting privacy settings, and thinking about what they share) and felt this would be good information for the government to share.

| | | |
|---|---|---|
| Level of Concern | Extremely concerned (7) | 10 of 63 |
| **Mean 4.9** | **Concerned (5-6)** | **31 of 63** |
| | Neither (4) | 10 of 63 |
| | Not concerned (2-3) | 12 of 63 |
| | Not at all concerned (1) | 0 of 63 |
| Benefits | ✓ Time-saving in that information is targeted to their preferences | |
| Concerns | ✗ Sense of powerlessness in that this issue is potentially too far gone now<br>✗ Identity theft, credit card fraud, computer hacking, security system failure<br>✗ List selling<br>✗ Sense that records and information are stored/kept in perpetuity<br>✗ Terms of agreement/policies are far too long (time-consuming) and complicated to read | |
| In their own words… | ***"I have concerns about my kids. I think older people tend to be more cautious and when you're younger, there's more that goes online. As kids grow, they can have a certain irresponsibility [before becoming an adult]. I don't think they're as proactive [with protecting their personal information]."***<br>***"I sort of expect I could get hacked in using the Internet. I pick and choose the organizations I deal with and what I give them."***<br>***"I think most companies try to be proactive, but the bad guys are advanced, too."*** | |

## THE BODY AS INFORMATION

***Synopsis***

Extracting information from the body has traditionally been limited to the field of medicine. However, increasingly, we are seeing the collection of this type of data for a wide range of commercial, recreational and forensic purposes. The following are just a few examples:

- Genetic testing for genealogical or ancestral research.
- Fingerprints to facilitate cashless payments for services or goods, or admission to facilities.
- Heartbeats as passwords for technological devices.
- Facial or voice recognition tools for identification.
- Wrist bands that track heart rates, exercise and sleep patterns.

The information generated by our bodies is uniquely personal, and as such it can be highly sensitive. As more and more information about our bodies is collected and digitized, particularly by non-medical organizations and individuals, the impacts on privacy must be considered.

Most are somewhat less concerned about this topic and didn't have any first-hand experience or knowledge of the examples provided. Participants believe the medical profession has a responsibility (and legal requirement) to protect personal information, and they trust them to uphold this responsibility. They feel this data is uniquely personal and, therefore, there is a greater sensitivity surrounding the storing or sharing of this information, especially with non-medical organizations, such as insurance companies. In many cases, participants believe that digitization of body information puts the security of the information at risk.

Those who are most concerned with this topic felt that personal information about the body is extremely sensitive and there should be strict controls over how and when it collected or shared. Those less concerned include participants who felt it was their choice as to whether they wanted to share this type of information. In terms of the use of fingerprints or voice recognition, participants often felt that using these measures increased protection and solved other problems, with passwords for example. Regardless, participants felt the protection of the information is of utmost importance as information about a person's body is viewed as the most personal type of information. Some participants felt that this issue is not prevalent in society now, but that it is likely to be a bigger concern in the future.

Most felt that privacy protection in this instance is shared: businesses and organizations (particularly medical) should be protecting the information already; government should ensure the proper checks and balances are in place and explore potential security breaches and safeguards; and individuals have a responsibility to understand what information they are sharing and how it will be used and stored, and from there it is up to them to determine whether they're comfortable or not.

| | | |
|---|---|---|
| Level of Concern | Extremely concerned (7) | 10 of 63 |
| **Mean 4.6** | **Concerned (5-6)** | **24 of 63** |
| | Neither (4) | 10 of 63 |
| | Not concerned (2-3) | 17 of 63 |
| | Not at all concerned (1) | 2 of 63 |
| Benefits | ✓ Increased security protection with unique passwords and identification<br>✓ Increased efficiencies and convenience (e.x., eye scan with Nexus) | |
| Concerns | ✗ Security of technology, computer hacking, etc.<br>✗ Someone's personal information being used by others to make decisions about them—personally or professionally<br>✗ Identity theft/fraud<br>✗ Information being misunderstood<br>✗ Information being accessed/shared without consent<br>✗ Information is very personal/sensitive (i.e. fingerprints, heartbeats, etc.) | |
| In their own words… | ***"My concern is whether they look at your medical history and reach conclusions. They form an idea, a prejudice. You can be denied employment."***<br>***"Information can be taken out of context."***<br>***"This info is a lot more difficult to duplicate in that a lot of these are unique to an individual. I'd feel more secure [if it was used for identity verification]."*** | |

## GOVERNMENT SURVEILLANCE

***Synopsis***

Governments around the world conduct surveillance and collect personal information in an effort to combat threats to security and safety. Advances in technology and ease with which data can be collected, stored and shared, has increased the technical capacity for surveillance exponentially, making it possible to collect personal information on far greater scales. For example, closed circuit televisions are a common sight, participants in large-scale events and protests can be monitored and identified, and unmanned aerial vehicles—also known as drones—are being used to patrol borders, monitor protests, and for investigative purposes. In addition, individuals are making more and more personal information accessible online (e.x., through social networking sites) and these data trails can paint detailed pictures of our lives.

This topic, perhaps more than others, raised the most concerns in terms of democracy, rights and freedoms. Participants feel that there is a fine line between conducting surveillance for reasons of national security and crime, and infringing on basic rights and freedoms. For the most part, participants are comfortable with surveillance for the protection of national security and crime prevention. Most expect (and some are comfortable with the idea) that they are being watched and recorded pretty much everywhere now, though the level of concern is higher regarding monitoring Internet activities, given that there is less understanding of why it would be done or what it is being used for. There is more concern about monitoring of peaceful protests. Protests are felt to be a right and a few participants worry about the infringement of their liberties (to travel for example) if they were videotaped and subsequently labeled as a result of participating in or observing a protest. A number of participants do believe the government should be open and transparent in informing Canadians about what is being checked and monitored, especially if they themselves are being monitored or investigated. While some feel that it may be inevitable to avoid monitoring presumably innocent people, they do not like the idea of being profiled without their knowledge given that there is little recourse to defend the data collected and how it may be interpreted.

In Montreal, there was more of a sense that while the government should be there for protection (e.x., surveillance for national security), it should not restrict the personal freedoms that participants enjoy.

Participants felt that the responsibility lies heavily on the government to properly store and protect the information gathered and to be cautious about how the information is used. Some participants felt that they had no choice to “opt out” as public surveillance is so prevalent and accepted in society.

| | | |
|---|---|---|
| Level of Concern<br>**Mean 4.5** | Extremely concerned (7) | 8 of 63 |
| | **Concerned (5-6)** | **30 of 63** |
| | Neither (4) | 10 of 63 |
| | Not concerned (2-3) | 12 of 63 |
| | Not at all concerned (1) | 3 of 63 |
| Benefits | ✓ Crime prevention and national security | |
| Concerns | ✗ Threat to democracy<br>✗ Profiling; info could be used to marginalize certain people or groups<br>✗ Decisions made about you<br>✗ Limit one's right to protest | |
| In their own words… | ***"This is a very slippery slope. Those who value security over freedom deserve neither."***<br>***"I think surveillance could be a deterrent to peaceful assembly."***<br>***"I think in some instances, it's helpful. Traffic cams can record accidents which can be helpful."***<br>***"It's for our own protection. An honest citizen doesn't worry about that."*** | |

## ECONOMICS OF PERSONAL INFORMATION

***Synopsis***

When we surf online or on our phone, we are enticed to sign up for the benefits of customer loyalty programs or to supply our contact information so that we won't miss the next big sale. Online, there are innumerable services applications that we can access for "free" (e.x., email, search engines, and social media sites), and data about our internet browsing habits is gathered to personalize our surfing experience. The unstated nature of these transactions is that users are trading their personal information (i.e. usage, contacts, interests) for benefits or access to services. Organizations, in turn, are able to use this information to discover potential customers, supply targeted advertisements, identify people who are likely to purchase their products, or sell it to other organizations. In essence, personal information has become a commodity—and finding ways to profit from our information has become a big business.

Most are aware of the privacy drawbacks of using online services and generally understand that free services are offered in exchange for personal information. The fact that companies use their personal information to send them tailored advertisements or market to their interests is known, and generally seen as an annoyance that can be ignored or mitigated by technology (e.x., advertisement blockers and spam filters) or by limiting behaviours (e.x., deleting spam emails without reading them).

Those not all that concerned with this topic believe they have control over their personal information in that they can limit their online behaviour and exposure. Some (the minority) also appreciate the service and welcome the convenience of receiving offers that they may be interested in.

For those concerned with this topic, the most important threat and the one that tends to curb most of their online behaviour is identity theft. Participants are worried about the potential long-term financial or reputational implications of this outcome. Many participants feel that companies should not be able to sell personal information and feel annoyed when they receive unwanted communications from organizations with whom they did not specifically share their personal information. Frustrations are felt by those who wish that they could go online without having their personal information collected.

Having said that, some participants weigh the pros and cons of providing personal information in exchange for monetary benefits or rewards. If they feel that there is sufficient personal benefit, then they will share their personal information.

For this topic, participants believe the onus is mostly on the individual to protect their personal privacy. Some feel that organizations and businesses have a role to play in protecting the personal information of their customers, but that they will only be as stringent as they are required by law. Participants would like to see more ethical business practices, and emphasized the importance of having the ability to opt-out of having their personal information collected or used. Other than setting regulations, most do not see a role for government in this area.

| | | |
|---|---|---|
| Level of Concern<br>**Mean 4.4** | Extremely concerned (7)<br>**Concerned (5-6)**<br>Neither (4)<br>Not concerned (2-3)<br>Not at all concerned (1) | 7 of 63<br>**23 of 63**<br>13 of 63<br>18 of 63<br>2 of 63 |
| Benefits | ✓ Membership rewards, deals, discounts | |
| Concerns | ✗ Pop-ups, targeted emails/offerings, frequent emails (SPAM)<br>✗ List selling<br>✗ Identity theft<br>✗ Limited freedom of choice (offers tailored to preferences) | |
| In their own words… | ***“It is more of an annoyance. [Social media website] is free. I’m not paying for it. I understand they use everything I say and do to send me specified ads.”***<br>***“We are bombarded and constantly solicited. The individual becomes the merchandise.”***<br>***“The part that bothers me is that it is brainwashing and conditioning us. They’re imposing ads, images, etc. on me that they think I am interested in. It limits my freedom of choice.”*** | |

## GOVERNMENT INFORMATION SHARING

***Synopsis***

As the Government of Canada seeks to improve programs and enhance service delivery, it is adopting new technologies and increasingly collecting and sharing digital data for an ever-broadening range of purposes. For example, some customs information collected from travelers returning to Canada by air is used to verify Employment Insurance claims. The government is consolidating the delivery of services through the creation of new departments like Service Canada. This approach can offer greater convenience but also requires increased sharing and linking of personal information.

Concern about privacy protection in this instance varied widely, with some participants having extreme concern and others having low or no concern. Those with higher levels of concern worry about the amount of information that government could compile on individuals if personal information held by various departments was more readily shared or centralized to make it more accessible. They are also concerned about the loss of personal control that may result from more sharing, and some argue it is an infringement of our civil liberties, rights and freedoms. For many, there is also a sense that government does not have the technical ability to properly protect personal information ("They're always behind the 8 ball") and some supported their opinion by citing recent government breaches. The concern is more about untrustworthy individuals seeking out this information rather than trust in the government itself.

Those with lower levels of concern feel that the government already has a lot of information about them (and that they have little choice in the matter) and they like the idea of improvements to government services that might be realized if departments and agencies were sharing information. If they could trust that the information was shared securely, these participants feel there would be efficiencies gained if information was accessible by (and only by) the government departments that needed it. When prompted, participants felt that they could trust the government to share the information properly, meaning only with the departments that needed it, at the appropriate times and in the right way. Participants were more concerned about the ability to share and store the data securely rather than the government's intention for collecting and using the data.

Most participants feel that the responsibility for the protection of personal information for this issue is mainly on the government to limit the data collected and to ensure that only pertinent information is shared and that it is stored securely.

| | | |
|---|---|---|
| Level of Concern<br>**Mean 4.3** | Extremely concerned (7) | 6 of 63 |
| | **Concerned (5-6)** | **29 of 63** |
| | Neither (4) | 6 of 63 |
| | Not concerned (2-3) | 18 of 63 |
| | Not at all concerned (1) | 4 of 63 |
| Benefits | ✓ Improved efficiency and government services<br>✓ Identify those abusing the system | |
| Concerns | ✗ Security of technology, computer, etc. hacking<br>✗ Lack of confidence in government's ability to protect personal information (particularly in terms of technology)<br>✗ Use of personal information without consent<br>✗ Decisions being made about you<br>✗ Threat to democracy<br>✗ Potential misinterpretation of personal information | |
| In their own words… | ***"I like the idea because it would result in less duplication."***<br>***"I am not confident the government has the most robust systems."***<br>***"If my information is being shared internationally or used against me, it's a concern."*** | |

## C. Responsibility for Privacy Protection

After the discussion about various privacy issues was complete, participants were asked to discuss responsibility for privacy protection in general. For this part of the discussion, most participants started from the premise that it is their responsibility to protect, monitor, and adapt their own behaviour to avoid negative consequences as best they can. This includes things such as: reading terms and conditions before engaging in services; only dealing with businesses, organizations, or websites that they trust; and only sharing the info that they feel comfortable with.

The next level of privacy protection should be provided by businesses and organizations. Participants expect that businesses will live up to certain standards of good business practices and ethics by protecting the information they collect, store, and use.

With respect to the government, participants believe the government's role is to ensure proper laws and regulations are in place and that businesses and organizations are monitored and penalized for breaches. If governments or organizations are collecting information, there is an expectation that they store and manage the information properly, and advise Canadians about how they use it, with whom it is shared and for what purpose. When asked specifically what government could and should be doing to protect privacy, participants suggested:

- Legislation/regulations governing privacy protection (privacy laws);
- Monitor and hold companies accountable for breaches;
- Sanction/penalize companies for privacy breaches;
- Establish a watchdog agency to monitor;
- Require companies to enforce frequent password changes;
- Update legislation/regulations frequently—ensure they keep up with evolving times;
- Inform/educate Canadians about the privacy laws currently in place;
- Ensure transparency; inform Canadians when they are being monitored, for what purpose and how;
- Inform Canadians or request approval to exchange their personal information (and identify with whom and for what purpose);
- Inform Canadians about any personal information stored out of country (and identify with which company the information is being stored and how it is protected);
- Cooperate with other governments/take part (or a leadership role) in global privacy community;
- Inform Canadians about privacy risks and educate them on how to protect themselves;
- Be open and transparent about the technology used to monitor Canadians (where it is and for what purpose); and
- Erase personal information that is no longer relevant.

## APPENDIX A: RECRUITMENT SCREENER

**Questionnaire #______________** **Date of Last Group_____________**
**# of previous groups____________**

| | |
|---|---|
| **Vancouver, BC**<br>**Wednesday, December 3**<br>**Group 1: General Population @ 5:30 pm $75**<br>**Group 2: Engaged Canadians @ 7:30 pm $75**<br><br>**Montreal, QC**<br>**Monday, December 8**<br>**Group 3: General Population @ 5:30 pm $75**<br>**Group 4: Engaged Canadians @ 7:30 pm $75**<br><br>**Halifax, NS**<br>**Tuesday, December 9**<br>**Group 5: General Population @ 5:30 pm $75**<br>**Group 6: Engaged Canadians @ 7:30 pm $75**<br><br>**Toronto, ON**<br>**Wednesday, December 10**<br>**Group 5: General Population @ 5:30 pm $75**<br>**Group 6: Engaged Canadians @ 7:30 pm $75** | Recruit: 10 for 8 to 10 to show per group<br><br>Honorarium:<br>$75<br><br>Study#: ###<br><br>Definitions:<br>General Population:<br>Half of the group should follow news or publicy policy somewhat or very closely.<br>Aim for mix of demographics.<br><br>Engaged Canadians:<br>Must follow news and public policy somewhat or very closely.<br>Aim for mix of demographics. |
| **Respondent's name:**<br>**Respondent's phone #: ________________________________ (home)**<br>**Respondent's phone #: ________________________________(work)**<br>**Respondent's fax #: ________________________sent?_____or**<br>**Respondent's e-mail : _______________________sent?**<br>**Sample source (circle): panel random client referral** | Interviewer:<br>Date:<br>Validated:<br>Quality Central:<br>On List:<br>On Quotas: |

Hello/Bonjour (pause), my name is ______________. Would you prefer to continue in English or French? / Préférez-vous continuer en anglais ou en français?

*[INTERVIEWER NOTE FOR ENGLISH GROUPS: IF PARTICIPANT WOULD PREFER TO CONTINUE IN FRENCH, PLEASE RESPOND WITH, "Malheureusement, nous recherchons des gens qui parlent anglais pour participer à ces groupes de discussion. Nous vous remercions de votre intérêt."]*

I'm calling from Nielsen Consumer Insights, a national public opinion research firm. We're organizing discussions on issues of importance to Canadians, on behalf of the Government of Canada. Up to 10 participants will be taking part and for their time, participants will receive an honorarium. May I ask you a few questions?

Yes **CONTINUE**
No **THANK AND TERMINATE**

Participation is voluntary. We are interested in hearing your opinions, no attempt will be made to sell you anything or change your point of view. The format is a "round table" discussion lead by a research professional. All opinions expressed will remain anonymous and views will be grouped together to ensure no particular individual can be identified.

**EXPLAIN FOCUS GROUPS**

About ten people will be taking part, all of them randomly recruited just like you. For their time, participants will receive an honorarium. But before we invite you to attend, we need to ask you a few questions to ensure that we get a good mix and variety of people. May I ask you a few questions?

Yes **CONTINUE**
No **ASK IF ANYONE ELSE IN THE HOUSEHOLD MIGHT BE INTERESTED**
***IF NOT THANK AND TERMINATE***

**READ TO ALL:** "This call may be monitored or audio taped for quality control and evaluation purposes. All audio tapes are destroyed after the evaluation"
**ADDITIONAL CLARIFICATION IF NEEDED:**

- to ensure that I (the interviewer) am reading the questions correctly and collecting your answers accurately;
- to assess my (the interviewer) work for performance evaluation;
- to ensure that the questionnaire is accurate/correct (i.e. evaluation of CATI programming and methodology – we're asking the right questions to meet our clients' research requirements – kind of like pre-testing).
- If the call is audio taped, it is only for the purposes of playback to the interviewer for a performance evaluation immediately after the interview is conducted or it can be used by the Project Manager/client to evaluate the questionnaire if they were unavailable at the time of the interview – all audio tapes are destroyed after the evaluation.

1. Do you or does any member of your household work…

| | Yes | No |
|---|---|---|

| | | |
|---|---|---|
| For a marketing research firm | **1** | **2** |
| For a magazine or newspaper, online or print | **1** | **2** |
| For a radio or television station | **1** | **2** |
| For a public relations company | **1** | **2** |
| For the government, whether federal or provincial | **1** | **2** |
| For an advertising agency or graphic design firm | **1** | **2** |
| For an online media company | **1** | **2** |

**IF "YES" TO ANY OF THE ABOVE, THANK AND TERMINATE**

2. On a scale of 1-5 where 1 is not at all closely and 5 is very closely, how closely do you follow news and public issues?

| | |
|---|---|
| 1 | Not at all closely |
| 2 | |
| 3 | |
| 4 | |
| 5 | Very closely |

3. On a scale of 1-5 where 1 is no interest and 5 is a lot of interest, how much interest do you take in politics and public policies?

| | |
|---|---|
| 1 | No interest |
| 2 | |
| 3 | |
| 4 | |
| 5 | A lot of interest |

| | |
|---|---|
| **General Population** | **Half of the group must say 3, 4 or 5 on either question 2 or 3.** |
| **Engaged Canadians** | **Must say 3, 4 or 5 on questions 2 and 3.** |

**[INTERVIEWER NOTE: CHECK PARTICIPANTS AVAILABILITY (DATE & TIME) BEFORE PROCEEDING. THIS IS NOT A FORMAL INVITATION.]**

4. Could you please tell me what age category you fall in to? Are you...

| | | |
|---|---|---|
| Under 18 | 0 | **THANK AND TERMINATE** |
| 18-34 years | 1 | 1 **ENSURE GOOD MIX PER GROUP** |
| 35-44 years | 2 | |
| 45-54 years | 3 | |
| 55-64 years | 4 | |
| 65 years or older | 5 | |
| Refuse | 9 | **THANK AND TERMINATE** |

5. What is your current employment status?

| | | |
|---|---|---|
| Working full-time | 1 | **ENSURE GOOD MIX PER GROUP** |
| Working part-time | 2 | |
| Self-employed | 3 | |
| Retired | 4 | |
| Unemployed | 5 | |
| Student | 6 | |
| Other | 7 | |
| DK/RF | 99 | |

6. Which of the following categories best describes your total household income? That is, the total income of all persons in your household combined, before taxes [READ LIST]?

| | | |
|---|---|---|
| Under $20,000 | 1 | **ENSURE GOOD MIX PER GROUP** |
| $20,000 to just under $ 40,000 | 2 | |
| $40,000 to just under $ 60,000 | 3 | |
| $60,000 to just under $ 80,000 | 4 | |
| $80,000 to just under $100,000 | 5 | |
| $100,000 to just under $150,000 | 6 | |
| $150,000 and above | 7 | |
| DK/RF | 99 | |

7. Could you please tell me what is the last level of education that you have completed?

| | | |
|---|---|---|
| Some high school only | 1 | ENSURE GOOD MIX |
| Completed high school | 2 | |
| Some College/University | 3 | |
| Completed College/University | 4 | |
| RF/DK | 9 | |

8. Are you a Canadian citizen at least 18 years old who normally resides in the [XX] area?

| | | |
|---|---|---|
| Yes | 1 | **CONTINUE** |
| No | 2 | **THANK AND TERMINATE** |

9. **DO NOT ASK – NOTE GENDER (TARGET 50/50 SPLIT)**

| | |
|---|---|
| Male | 1 |
| Female | 2 |

10. Have you ever attended a consumer group discussion, an interview or survey which was arranged in advance and for which you received a sum of money?

| | | |
|---|---|---|
| Yes | 1 | **MAX. 2/3 PER GROUP** |
| No | 2 | **GO TO Q11** |

11. How long ago was it? ____________________________

**TERMINATE IF IN THE PAST 6 MONTHS**

12. How many consumer discussion groups have you attended in the past 5 years?

____________________________

**TERMINATE IF MORE THAN 5 DISCUSSION GROUPS**

13. Sometimes participants are also asked to write out their answers to a questionnaire, read materials or watch TV commercials during the discussion. Is there any reason why you could not participate? [READ IF NEEDED: I can assure you that everything written or discussed in the groups will remain confidential]

| | | |
|---|---|---|
| Yes | 1 | **THANK & TERMINATE** |
| No | 2 | **CONTINUE TO PRIVACY QUESTIONS** |

**[INTERVIEWER NOTE: TERMINATE IF RESPONDENT OFFERS ANY REASON SUCH AS SIGHT OR HEARING PROBLEM, A WRITTEN OR VERBAL LANGUAGE PROBLEM, A CONCERN WITH NOT BEING ABLE TO COMMUNICATE EFFECTIVELY OR IF YOU HAVE A CONCERN.]**

**PRIVACY QUESTIONS**

Now I have a few questions that relate to privacy, your personal information and the research process. We will need your consent on a few issues that enable us to conduct our research. As I run through these questions, please feel free to ask me any questions you would like clarified.

P1) First, we will be providing the hosting facility and session moderator with a list of respondents' names and profiles (screener responses) so that they can sign you into the group. Do we have your permission to do this? I assure you it will be kept strictly confidential.

| | | |
|---|---|---|
| Yes | 1 | **GO TO P2** |
| No | 2 | **READ RESPONDENT INFO BELOW** |

**READ ONLY IF SAYS NO AT P1.** We need to provide the facility hosting the session and the moderator with the names and background of the people attending the focus group because only the individuals invited are allowed in the session and the facility and moderator must have this information for verification purposes. Please be assured that this information will be kept strictly confidential. **GO TO P1A**

P1a) Now that I've explained this, do I have your permission to provide your name and profile to the facility?

| | | |
|---|---|---|
| Yes | 1 | **GO TO P2** |
| No | 2 | **THANK & TERMINATE** |

P2) As well, an audio and/or video tape of the group session will be produced for research purposes. The tapes will be used by the research professional to assist in preparing a report on the research findings and will be destroyed once the final report is completed (no later than the end of March 2015). Additionally, the client will receive a copy of the tapes, so that they can observe the focus group discussions. However, the client will not receive personally identifiable information, such as your full name or contact information, and the client will destroy the tapes at the conclusion of the project (no later than the end of March 2015). Do you agree to be audio and/or video taped for research purposes only?

| | | |
|---|---|---|
| Yes | 1 | **THANK & GO TO P3** |
| No | 2 | **READ RESPONDENT INFO BELOW** |

**READ ONLY IF SAYS NO AT P2.** It is necessary for the research process for us to audio/video tape the session as the researcher needs this material to complete the report. The client has provided written consent that the recording will be used for the intended purpose of the research and for internal use only. I assure you it is kept strictly confidential and it will be destroyed as when the research is complete. **GO TO P2A**

P2a) Now that I've explained this, do I have your permission for audio/video taping?

| | | |
|---|---|---|
| Yes | 1 | **THANK & GO TO P3** |
| No | 2 | **THANK AND TERMINATE** |

P3) Each month FocusSearch submits the names of individuals that have participated in our focus groups to the Marketing Research and Intelligence Association Qualitative Central system (www.mria-arim.ca). Qualitative Central serves as a centralized database to review participation in qualitative research and focus groups. You will not be contacted for any reason whatsoever as a result of being on this list.

Do we have your permission to submit your name and phone number to MRIA's Qualitative Central system?

| | | |
|---|---|---|
| Yes | 1 | **THANK & GO TO INVITATION** |
| No | 2 | **GO TO P3A** |

P3a) **READ ONLY IF SAYS NO AT P3.** To participate in this focus group we must have your permission to add your name to the Qualitative Central system as it is the only way for us to ensure the integrity of the research process and track participation in qualitative research. The system is maintained by the industry body, the Marketing Research and Intelligence Association, and is solely used to track your participation in qualitative research (such as focus groups). You will not be contacted for any reason whatsoever as a result of being on this list.

Now that I've explained this do I have your permission to add your name to our qualitative central list?

| | | |
|---|---|---|
| Yes | 1 | **THANK & GO TO INVITATION** |
| No | 2 | **THANK & TERMINATE** |

**AS REQUIRED, ADDITIONAL INFO FOR THE INTERVIEWER:**

Please be assured that this information is kept confidential and is strictly accessed and used by professional market research firm to review participation and prevent "professional respondents" from attending sessions. Research firms participating in MRIA's Qualitative Central require your consent to be eligible to participate in the focus group - the system helps ensure the integrity of the research process.

**AS REQUIRED, NOTE ABOUT MRIA:**

The Marketing Research and Intelligence Association is a non-profit organization for marketing research professionals engaged in marketing, advertising, social, and political research. The Society's mission is to be the leader in promoting excellence in the practice of marketing and social research and in the value of market information.

**INVITATION**

As I mentioned earlier, the group discussion will take place on **DATE @ TIME for 2 hours** and participants will receive **$75** for their time. To confirm, are you able to attend?

| | | |
|---|---|---|
| Yes | 1 | **CONTINUE** |
| No | 2 | **THANK AND TERMINATE** |

Do you have a pen handy so that I can give you the address where the group will be held? It will be held at:

| | |
|---|---|
| **Vancouver, BC**<br>Wednesday, December 3<br>FACILITY TBD | **Montreal, QC**<br>Monday, December 8<br>FACILITY TBD |
| **Halifax, NS**<br>Tuesday, December 9<br>FACILITY TBD | **Toronto, ON**<br>Wednesday, December 10<br>FACILITY TBD |

We ask that you arrive fifteen minutes early to be sure you find parking, locate the facility and have time to check-in with the hosts. The hosts may be checking respondents' identification prior to the group, so please be sure to bring some personal identification with you (for example, a driver's license). If you require glasses for reading make sure you bring them with you as well.

As we are only inviting a small number of people, your participation is very important to us. If for some reason you are unable to attend, please call us so that we may get someone to replace you. You can reach us at **[1-800 NUMBER]** at our office. Please ask for **[NAME].** Someone will call you the day before to remind you about the discussion.

So that we can call you to remind you about the focus group or contact you should there be any changes, can you please confirm your name and contact information for me? **[TO BE COLLECTED UPON FORMAL INVITATION ONLY SO AS NOT TO COLLECT PERSONAL INFORMATION UNNECESSARILY.]**

First name________________________________________________
Last Name________________________________________________
Email______________________________________________________
Daytime phone number_________________________________
Evening phone number_________________________________

**If the respondent refuses to give his/her first or last name or phone number please assure them that this information will be kept strictly confidential in accordance with the privacy law and that it is used strictly to contact them to confirm their attendance and to inform them of any changes to the focus group. If they still refuse THANK & TERMINATE.**

# APPENDIX B: DISCUSSION GUIDE

## INTRODUCTION AND WARM-UP (5 MINUTES)

Welcome participants and explain the process:

- Moderator introduces him/herself and his/her role
- The role of moderator is to ask questions, make sure everyone has a chance to express themselves, keep track of the time, be objective/no special interest
- Role of participants: speak openly and frankly about opinions, remember that there are no right or wrong answers and no need to agree with each other
- Results are confidential and reported all together/individuals are not identified/participation is voluntary
- Audio and video taping of the discussion, one-way mirror and colleagues viewing in the back room
- Turn off cell phones for the duration of the discussion
- *To start, I'd like to go around the room and ask each of your to introduce yourself. Please tell us your name, what you do during the day and also… Our discussion today/tonight is going to focus on privacy. Protecting privacy means different things to different people. As part of your introduction, tell us what privacy means to you.*

## GENERAL KNOWLEDGE AND CONCERN ABOUT PRIVACY (20 MINUTES)

As mentioned, we're going to be discussing privacy and specifically your personal privacy and the protection of your personal information. Personal information includes things like your name, age, address, income and email address, but also information like your opinions, purchasing habits, online activities, even your DNA; things like that.

- How much do you generally care about your privacy? Would you say it's something that concerns you very much or not all that much? Why/why not?
- What are you most concerned about?
  - PROBE WITH: Stalking? Marketing? Employment risks? Security breaches? Identity theft? Credit Cards? Hacking? Embarrassment? Social surveillance (e.x., protesters) Decisions being made about you – personally or professionally? Others using your personal information without your consent?
- What do you do, or not do, as a result of this concern? Have you changed your habits in any way as a result of a concern about your privacy?
  - What measures have you taken?
- Do you feel that you have control over the information that you share? Why/Why not?
- (IF YES) Which assurances have you been given that make you feel confident that your privacy (personal information) is being protected or safeguarded?

- Our definition of privacy and concern vary depending on situations and the type of transactions. Tell me more about what types of organizations you trust the most with your personal information? Which ones do you trust the least? And why?
- What about in terms of your privacy online versus offline? Do you have similar concerns for both or is your level of concern different? If so, in what ways? Please explain.
- Thinking about the various things you do online whether using a smartphone, tablet, computer or other electronic/internet-enabled device, what specific online activities concern you in terms of your privacy? Which activities do not?

  (IF NEEDED PROBE WITH THESE CONCEPTS BUT AVOID USING SPECIFIC COMPANY NAMES)

  - Banking
  - Shopping online
  - Online auctions
  - Social media
  - Emails
  - Online classifieds
  - Websites
  - Registering software online
  - Use your phone for navigational/GPS information

## EXPLORATION OF PROPOSED PRIVACY PRIORITIES (80 MINUTES)

I would like to turn to a few specific areas of exploration. I will provide a brief description of each which I will ask you to read and then we will follow-up with a group discussion for each.

The first issue we are going to look at tonight is…

*MODERATOR DISTRIBUTES HANDOUT SUMMARIZING THE ISSUE TO EACH PARTICIPANT. MODERATOR WILL ASK PARTICIPANTS TO REVIEW INDEPENDENTLY AND MAKE ANY COMMENTS ON IT. MODERATOR WILL ASK THEM TO IDENTIFY THE THREE THINGS THAT STOOD OUT THE MOST TO THEM WHILE THEY WERE REVIEWING.*

Take a couple minutes to digest the information. What we present here is a visual which is meant to spark conversation but that may only represent certain aspects of the issue and a description which gives more information about the full topic. Feel free to write on it; circle anything that stands out for you (either positively or negatively). For each one, you will also be asked to complete two exercises. First, indicate how concerned you are about the protection of your privacy on a scale of 1 to 7, where ‘1’ means not concerned at all, and ‘7’ means extremely concerned. Second, write down your concerns with respect to privacy related to this area. Please do this independently as we will discuss together as a group once you’re all done.

| Discussion Order | Vancouver, BC | Montreal, QC | Halifax, NS | Toronto, ON |
|---|---|---|---|---|
| Group 1: General Population | A | G | B | E |

| | | | | |
|---|---|---|---|---|
| | B<br>C<br>D<br>E<br>F<br>G | F<br>E<br>D<br>C<br>B<br>A | D<br>F<br>A<br>C<br>E<br>G | C<br>A<br>G<br>F<br>D<br>B |
| Group 2: Engaged Canadians | D<br>E<br>F<br>G<br>A<br>B<br>C | C<br>B<br>A<br>G<br>F<br>E<br>D | F<br>C<br>E<br>B<br>G<br>D<br>A | A<br>G<br>B<br>F<br>D<br>C<br>E |

### *A. Economics of Personal Information*

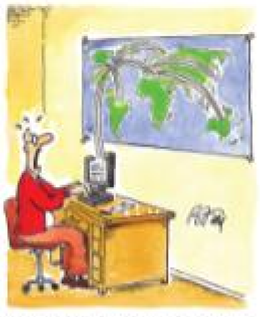
"HOW WOULD YOU LIKE TO PAY FOR YOUR PURCHASE TODAY– CASH, CREDIT OR PERSONAL INFORMATION?"

When we surf online or on our phone, we are enticed to sign up for the benefits of customer loyalty programs or to supply our contact information so that we won't miss the next big sale. Online, there are innumerable services applications that we can access for "free" (e.x., email, search engines, and social media sites), and data about our internet browsing habits is gathered to personalize our surfing experience. The unstated nature of these transactions is that users are trading their personal information (i.e. usage, contacts, interests) for benefits or access to services. Organizations, in turn, are able to use this information to discover potential customers, supply targeted advertisements, identify people who are likely to purchase their products, or sell it to other organizations. In essence, personal information has become a commodity—and finding ways to profit from our information has become a big business.

***Topics for discussion***

- Is this an issue that you have thought about before? Please explain.
- Does this issue bring anything to mind for you regarding the protection of your privacy? Why or why not?
- If there are concerns, what are they? Are there any others? Do the concerns outweigh the benefits?
- When you share your personal information, do you think about its value? How so?
- How willing are you to trade personal information for goods, services or benefits? Why/why not? Do you think you get good value for sharing your personal information?
- Would you be willing to share the following types of data with a company if there was a benefit to you, such as reward points or discounts/promotions? Why/Why not?
  - Data about where you shop and what you buy
  - Location data such as the places you have been
  - Financial data such as bank account and credit card details
  - Personal data such as your name, mailing address or telephone number
  - Health information
- What would you think if you found out that you were denied a service (e.x., insurance) or missed out on deals because you were not considered "desirable" by certain advertisers? If you had concerns, who would you turn to for help?
- Are you aware that organizations can use data about users' online activities to provide them with targeted advertising or personalized content? How do you feel about this? Do you think this is useful or does it make you feel like you have less privacy online?
- Do you have concerns about organizations using your personal information to generate their own revenue?
- Now that you've had a chance to think about privacy from this perspective, does this change the way you feel about providing personal information? How so?
- Thinking about this issue, who do you think is primarily responsible for making sure personal information is protected – individuals, organizations, government? How so?

### B. *Protecting Canadians in a Borderless World*



"IF ONLY I COULD GET FREQUENT FLYER MILES FOR THE TRAVELS OF MY PERSONAL INFORMATION."

In a globally networked and integrated economy, personal information and data can move quickly and effortlessly around the globe:

- Individuals use cloud services for photo sharing, social networking or email, and shop online with businesses based in other countries.
- Businesses may transfer the personal information they collect to organizations in other countries for processing or storage.
- Governments share personal information with other countries for law enforcement and security purposes.

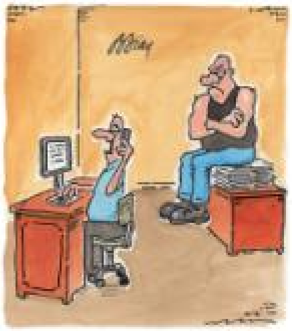
When data moves around the world, it can end up in countries that have weak privacy protections or none at all.

When data is collected by companies operating in many countries, data breaches or changes to terms and conditions or policies can impact individuals around the globe.

***Topics for discussion***

- Is this an issue that you have thought about before? Please explain.
- Does this issue bring anything to mind for you regarding the protection of your privacy? Why or why not?
- Do you feel your personal information is relatively well protected when it is held within Canada?
- Do you have any concerns about sharing your personal information with organizations (i.e. businesses and government) outside of Canada?
- Now that you've had a chance to think about privacy from this perspective, does this change the way you feel about providing personal information? How so?
- Thinking about this issue, who do you think is primarily responsible for making sure personal information is protected – individuals, organizations, governments? How so?

### *C. Strengthening Accountability & Privacy Safeguards*



"I CAN ASSURE YOU THAT OUR CONCERN FOR PROTECTING PERSONAL INFORMATION IS VERY DEEP-SEATED!"

Organizations have a responsibility to protect the personal information in their care. As more and more information is collected, processed and stored electronically, organizations must continually update their privacy practices and security measures to ensure that personal information will not be stolen, misused, leaked or lost. Organizations also need to clearly and proactively explain what personal information is collected, how it will be used and if it will be shared with any other organizations.

Individuals can take steps to improve their own privacy management practices by adopting good security practices (e.x., passwords), reading privacy policies and user agreements, adjusting privacy settings, and thinking carefully about the information they share or post about themselves and others.

***Topics for discussion***

- Do you think organizations (businesses and government) take their responsibilities to protect personal information seriously?
- Do you think organizations are proactive about protecting privacy or do you think they are more reactive? Why?
- Are you concerned about your personal information being lost, stolen or mistakenly disclosed by an organization that holds it? Why?
- What kinds of organizations do you trust the most with your personal information? Why?
- Which ones do you trust the least? Why?
- If you wanted to know what an organization is going to do with your personal information, where would you expect to find or get that information?
- Do you read privacy policies or user agreements? If no, why not? If yes, do you generally find them useful?
- What are the main factors you consider when deciding whether to share your personal information with an organization?
- Have you ever asked an organization (business or government) how your information is being used, handled or stored? Or refused to share your personal information? What made you take this action? Why have you not taken this action?
- Have you ever chosen not to do business or interact with an organization because you were unhappy or uncomfortable with the way it handles personal information? What was your concern? Do you take steps to protect your personal information? If so, what are some examples?
- Now that you've had a chance to think about privacy from this perspective, does this change the way you feel about providing personal information? How so?
- Thinking about this issue, who do you think is primarily responsible for making sure personal information is protected – individuals, organizations, governments? How so?

### *D. Government Information Sharing*

As the Government of Canada seeks to improve programs and enhance service delivery, it is adopting new technologies and increasingly collecting and sharing digital data for an ever-broadening range of purposes. For example, some customs information collected from travelers returning to Canada by air is used to verify Employment Insurance claims. The government is consolidating the delivery of services through the creation of new departments like Service Canada. This approach can offer greater convenience but also requires increased sharing and linking of personal information.

***Topics for discussion***

- Does it raise any concerns for you with respect to privacy? Why or why not?
- If there are concerns, what are they? Are there any others?
- Have you ever asked a government organization how your information is being used, handled or stored? What made you take this action? Why have you not taken this action?
- How comfortable are you with increased personal information sharing within the government? Why? How do you feel about the government sharing personal information with private-sector organizations?
- How comfortable or uncomfortable are you with government departments and agencies doing the following? [PROBE: Why is that?]
    - Sharing personal information collected at borders and airports with foreign governments. What about with other Canadian government departments or agencies?
- Are you confident that the government generally ensures that the personal information it holds has been shared with the right organization, in the correct way, and for the appropriate purpose? Why?

### *E. Government Surveillance*

Governments around the world conduct surveillance and collect personal information in an effort to combat threats to security and safety. Advances in technology and ease with which data can be collected, stored and shared, has increased the technical capacity for surveillance exponentially, making it possible to collect personal information on far greater scales. For example, closed circuit televisions are a common sight, participants in large-scale events and protests can be monitored and identified, and unmanned aerial vehicles—also known as drones—are being used to patrol borders, monitor protests, and for investigative purposes. In addition, individuals are making more and more personal information accessible online (e.x., through social networking sites) and these data trails can paint detailed pictures of our lives.

***Topics for discussion***

- How aware are you of government surveillance?
- How much do you understand about what information is collected, used, or disclosed by intelligence gathering activities in Canada?
- Do you think these agencies should have to explain their activities to Canadians and how they affect the privacy of Canadians? How comfortable or uncomfortable are you with government departments and agencies doing the following? [PROBE: Why is that?]
    - Using unmanned aerial vehicles, or drones, to conduct border surveillance. What about to conduct general surveillance over protests? Why?
    - Using audio or video surveillance cameras in public places for the purposes of law enforcement and public safety? Why?
    - Requesting telecommunications companies to provide personal information they hold about individuals without a warrant?
- What do you think about the statement: “If you have nothing to hide, you have nothing to fear.”?
- Now that you’ve had a chance to think about privacy from this perspective, does this change the way you feel about providing personal information? How so?

### *F. Reputation & Privacy*

"I'D LIKE TO HIRE YOU, BUT ACCORDING TO YOUR SURFING HABITS, YOU'RE A DOG PERSON AND WE'RE ALL CAT PEOPLE HERE!"

Our reputations reflect how others perceive us—and they can affect us both personally and professionally. The Internet has had a profound impact on personal reputation management. On the Internet, we shape our reputation by posting social media profiles, photos, online comments, etc. Our digital trails can also paint a picture of us—the sites we visit, where we shop, and our movements via the GPS on our phones. But others can shape our reputation as well by posting information about us.

Personal information can be easily posted, duplicated and shared on the web, but it can also be challenging to remove, correct or control.

***Topics for discussion***

- Is this an issue that you have thought about before? Please explain.
- Does this issue bring anything to mind for you regarding the protection of your privacy? Why or why not?
- If there are concerns, what are they? Are there any others?
- Do you post or share personal information about yourself online? What type of information are you comfortable posting or sharing?
- Do you post your comments, opinions, ideas or beliefs on the Internet? If so, do you identify yourself? Are you concerned about how these comments could be used by others to make decisions about you?
- Do you post information about other people? If so, what type of information? Have your posts about others ever impacted their lives?
- Do you take any steps to protect your reputation online?
- Have you ever used a search engine to see what information about you is online?
- Have you ever had anything posted online about you that negatively affected your life in any way – personally or professionally? What action did you take as a result? Was the issue resolved to your satisfaction?
- Have you ever used a search engine to find out more about someone you met? Did you trust the information that you found?
- Now that you've had a chance to think about privacy from this perspective, does this change the way you feel about posting personal information? How so?
- Thinking about this issue, who do you think is primarily responsible for making sure personal information is protected online – individuals, organizations, governments? How so?

### G. *The Body as Information*

"IT'S JUST A LITTLE TEST WE GIVE TO ALL OUR JOB APPLICANTS. THERE'S A PENCIL, SOME PAPER AND THAT LITTLE CUP IS FOR A URINE SAMPLE!"

Extracting information from the body has traditionally been limited to the field of medicine. However, increasingly, we are seeing the collection of this type of data for a wide range of commercial, recreational and forensic purposes. The following are just a few examples:

- Genetic testing for genealogical or ancestral research.
- Fingerprints to facilitate cashless payments for services or goods, or admission to facilities.
- Heartbeats as passwords for technological devices.
- Facial or voice recognition tools for identification.
- Wrist bands that track heart rates, exercise and sleep patterns.

The information generated by our bodies is uniquely personal, and as such it can be highly sensitive. As more and more information about our bodies is collected and digitized, particularly by non-medical organizations and individuals, the impacts on privacy must be considered.

***Topics for discussion***

- Is this an issue that you have thought about before? Please explain.
- Does this issue bring anything to mind for you regarding the protection of your privacy? Why or why not?
- If there are concerns, what are they? Are there any others?
- How do you feel about sharing information about your body with organizations (i.e. businesses or government)?
- What factors influence your decision to share personal information? Probe for: convenience, health benefits, better service, etc.?
- Are you concerned about the potential for information about your body being used by organizations outside of the medical field to make decisions about you? Why/why not?
- How concerned for your personal privacy are you with wearing computers, such as smart watches, pedometers and heart monitors that collect personal information about you? Have you taken any action as a result of these concerns?
- How concerned for you about your genetic information being used for non-health related purposes, such as determining eligibility for insurance or employment? What could be done to mitigate this concern?
- Now that you've had a chance to think about privacy from this perspective, does this change the way you feel about providing personal information? How so?
- Thinking about this issue, who do you think is primarily responsible for making sure personal information is protected online – individuals, organizations, governments? How so?

## WRAP-UP (10 MINUTES)

- Before we move on, we have covered a lot of ground in terms of exploring some new areas. Thinking about the seven areas we covered here tonight, which would you say are your top 3 privacy concerns? Which of the areas do you think are the most important? Why do you say that?

- What do you think the government could (or should) do to address/alleviate your privacy concerns? What about businesses? Why do you say that?
- Have you ever looked for information about your privacy rights? Why/why not?
- Where did/would you go for this information?

## CONCLUSION  (5 MINUTES)

*MODERATOR WILL GO BACK TO THE VIEWING ROOM TO SEE IF THERE ARE ANY ADDITIONAL QUESTIONS PRIOR TO CONCLUDING THE DISCUSSION.*

- This concludes what we needed to cover tonight. We really appreciate you taking the time to come down here and share your views. Your input is very important and insightful.
- Please leave all papers on the table.
- Don’t forget to see our host before you leave to receive your incentive. Good night!
- **GROUP 1:** Remind participants not to talk about the discussion to ensure second group doesn’t have any “hints” coming in.

# APPENDIX C: FOCUS GROUP HANDOUTS

## A. ECONOMICS OF PERSONAL INFORMATION

When we surf online or on our phone, we are enticed to sign up for the benefits of customer loyalty programs or to supply our contact information so that we won't miss the next big sale.

Online, there are innumerable services applications that we can access for "free" (e.x., email, search engines, and social media sites), and data about our internet browsing habits is gathered to personalize our surfing experience.

The unstated nature of these transactions is that users are trading their personal information (i.e. usage, contacts, interests) for benefits or access to services.

Organizations, in turn, are able to use this information to discover potential customers, supply targeted advertisements, identify people who are likely to purchase their products, or sell it to other organizations. In essence, personal information has become a commodity—and finding ways to profit from our information has become a big business.

" HOW WOULD YOU LIKE TO PAY FOR YOUR PURCHASE TODAY - CASH, CREDIT OR PERSONAL INFORMATION? "

**How concerned are you about the protection of your privacy related to this area?** *Please circle one.*

1 2 3 4 5 6 7

*Not at all Concerned* *Extremely Concerned*

**What are your concerns with respect to privacy related to this area?**

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

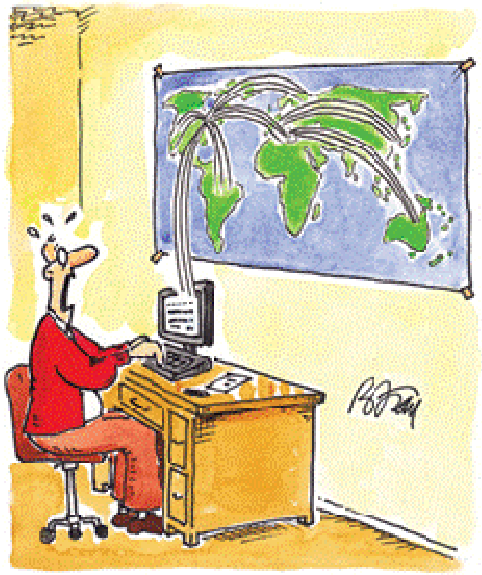
______________________________________________________________________________

## B. PROTECTING CANADIANS IN A BORDERLESS WORLD

In a globally networked and integrated economy, personal information and data can move quickly and effortlessly around the globe:

- Individuals use cloud services for photo sharing, social networking or email, and shop online with businesses based in other countries.
- Businesses may transfer the personal information they collect to organizations in other countries for processing or storage.
- Governments share personal information with other countries for law enforcement and security purposes.

When data moves around the world, it can end up in countries that have weak privacy protections or none at all. When data is collected by companies operating in many countries, data breaches or changes to terms and conditions or policies can impact individuals around the globe.



"IF ONLY I COULD GET FREQUENT FLYER MILES FOR THE TRAVELS OF MY PERSONAL INFORMATION!"

**How concerned are you about the protection of your privacy related to this area?** *Please circle one.*

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| *Not at all Concerned* | | | | | | *Extremely Concerned* |

**What are your concerns with respect to privacy related to this area?**

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

## C. STRENGTHENING ACCOUNTABILITY & PRIVACY SAFEGUARDS

Organizations have a responsibility to protect the personal information in their care. As more and more information is collected, processed and stored electronically, organizations must continually update their privacy practices and security measures to ensure that personal information will not be stolen, misused, leaked or lost. Organizations also need to clearly and proactively explain what personal information is collected, how it will be used and if it will be shared with any other organizations.

Individuals can take steps to improve their own privacy management practices by adopting good security practices (e.x., passwords), reading privacy policies and user agreements, adjusting privacy settings, and thinking carefully about the information they share or post about themselves and others.

"I CAN ASSURE YOU THAT OUR CONCERN FOR PROTECTING PERSONAL INFORMATION IS VERY DEEP-SEATED!"

**How concerned are you about the protection of your privacy related to this area?** *Please circle one.*

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| *Not at all Concerned* | | | | | | *Extremely Concerned* |

**What are your concerns with respect to privacy related to this area?**

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

## D. GOVERNMENT INFORMATION SHARING

As the Government of Canada seeks to improve programs and enhance service delivery, it is adopting new technologies and increasingly collecting and sharing digital data for an ever-broadening range of purposes. For example, some customs information collected from travelers returning to Canada by air is used to verify Employment Insurance claims. The government is consolidating the delivery of services through the creation of new departments like Service Canada. This approach can offer greater convenience but also requires increased sharing and linking of personal information.

---

**How concerned are you about the protection of your privacy related to this area?** *Please circle one.*

1 2 3 4 5 6 7

*Not at all Concerned* *Extremely Concerned*

**What are your concerns with respect to privacy related to this area?**

________________________________________________________________________________

________________________________________________________________________________

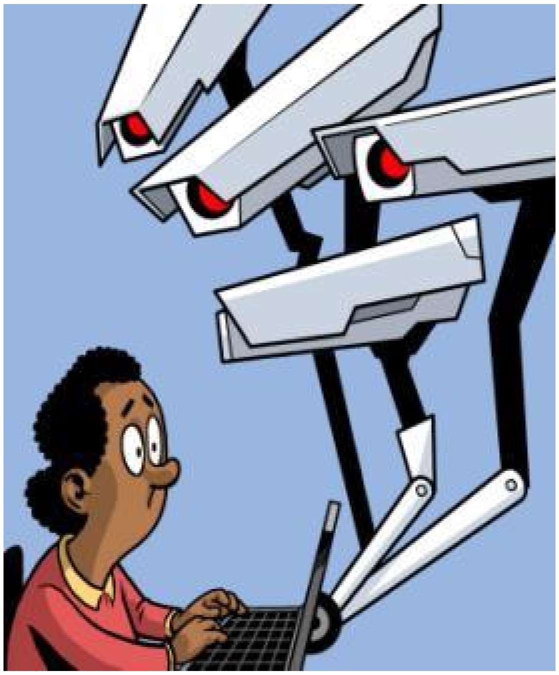
________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

## E. GOVERNMENT SURVEILLANCE

Governments around the world conduct surveillance and collect personal information in an effort to combat threats to security and safety. Advances in technology and ease with which data can be collected, stored and shared, has increased the technical capacity for surveillance exponentially, making it possible to collect personal information on far greater scales. For example, closed circuit televisions are a common sight, participants in large-scale events and protests can be monitored and identified, and unmanned aerial vehicles—also known as drones—are being used to patrol borders, monitor protests, and for investigative purposes. In addition, individuals are making more and more personal information accessible online (e.x., through social networking sites) and these data trails can paint detailed pictures of our lives.



**How concerned are you about the protection of your privacy related to this area?** *Please circle one.*

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| *Not at all Concerned* | | | | | | *Extremely Concerned* |

**What are your concerns with respect to privacy related to this area?**

_____________________________________________________________________________

_____________________________________________________________________________

_____________________________________________________________________________

_____________________________________________________________________________

_____________________________________________________________________________

## F. REPUTATION & PRIVACY

Our reputations reflect how others perceive us—and they can affect us both personally and professionally.

The Internet has had a profound impact on personal reputation management. On the Internet, we shape our reputation by posting social media profiles, photos, online comments, etc. Our digital trails can also paint a picture of us—the sites we visit, where we shop, and our movements via the GPS on our phones.

But others can shape our reputation as well by posting information about us. Personal information can be easily posted, duplicated and shared on the web, but it can also be challenging to remove, correct or control.

"I'D LIKE TO HIRE YOU, BUT ACCORDING TO YOUR SURFING HABITS, YOU'RE A DOG PERSON AND WE'RE ALL CAT PEOPLE HERE!"

**How concerned are you about the protection of your privacy related to this area?** *Please circle one.*

1 2 3 4 5 6 7

*Not at all Concerned* *Extremely Concerned*

**What are your concerns with respect to privacy related to this area?**

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

## G. THE BODY AS INFORMATION

Extracting information from the body has traditionally been limited to the field of medicine. However, increasingly, we are seeing the collection of this type of data for a wide range of commercial, recreational and forensic purposes. The following are just a few examples:

- Genetic testing for genealogical or ancestral research.
- Fingerprints to facilitate cashless payments for services or goods, or admission to facilities.
- Heartbeats as passwords for technological devices.
- Facial or voice recognition tools for identification.

"IT'S JUST A LITTLE TEST WE GIVE TO ALL OUR JOB APPLICANTS. THERE'S A PENCIL, SOME PAPER AND THAT LITTLE CUP IS FOR A URINE SAMPLE!"

- Wrist bands that track heart rates, exercise and sleep patterns.

The information generated by our bodies is uniquely personal, and as such it can be highly sensitive. As more and more information about our bodies is collected and digitized, particularly by non-medical organizations and individuals, the impacts on privacy must be considered.

---

**How concerned are you about the protection of your privacy related to this area?** *Please circle one.*

1 2 3 4 5 6 7

*Not at all Concerned* *Extremely Concerned*

**What are your concerns with respect to privacy related to this area?**

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

## About Nielsen

Nielsen Holdings N.V. (NYSE: NLSN) is a global information and measurement company with leading market positions in marketing and consumer information, television and other media measurement, online intelligence, mobile measurement, trade shows and related properties. Nielsen has a presence in approximately 100 countries, with headquarters in New York, USA and Diemen, the Netherlands. For more information, visit www.nielsen.com.