POR Number: POR 028-15
Contract Number: 2R008-150157/001/CY
Award Date: 2015-11-10
Contract Amount: $103,998.42

Final Report

2015-2016 Public Opinion Research with Canadian Businesses on Privacy-Related Issues (focus group discussions)

Qualitative Component: Focus Group Findings

Prepared for Office of the Privacy Commissioner of Canada

March 2016

Phoenix SPI is a 'Gold Seal Certified' Corporate Member of the MRIA

1678 Bank Street, Suite 2, Ottawa, ON, K1V 7Y6 T 613-260-1700 F 613-260-1300 E info@phoenixspi.ca
www.phoenixspi.ca

Table of Contents

Executive Summary

The Office of the Privacy Commissioner of Canada (OPC) commissioned Phoenix Strategic Perspectives Inc. (Phoenix) to conduct quantitative and qualitative opinion research with Canadian businesses on privacy-related issues. The purpose of the research was to better understand: 1) the extent to which businesses are familiar with privacy issues and requirements; and 2) the types of privacy policies and practices that they have in place. This report presents the findings from the qualitative research: a set of six focus groups held February 9-10, 2016 in Toronto, Moncton (conducted in French), and Winnipeg.

Contextual Information

Participants tend to deal with the collection, management and disposal of customer information. They devote limited time to privacy issues in their daily work activities and few have sought advice or received training on how to deal with privacy issues.

The types of privacy issues with which participants personally deal tend to fall into three categories, with participants sometimes having responsibilities in more than one area: 1) collecting information from customers (including updating information, obtaining consent to collect it, and explaining how it will be used); 2) managing the use, disclosure, and retention of information (including ensuring proper storage, managing/limiting access, and ensuring information is retained for the required/stipulated length of time); 3) disposing of customer information, which typically involves sending information for off-site storage and/or destruction of collected information. These responsibilities typically include ensuring compliance with company security practices/safeguards governing the collection, use, retention, and disposal of customer information.

The proportion of time typically devoted to privacy issues tends to be quite limited, a majority of participants estimating that it takes up no more than 5% of their time. Most of those who said they devote more time to such issues estimated that it was in the range of 5-10%. Very few recall having looked for advice to help them with privacy issues. Those who have sought advice have done so in relation to specific issues, including retention of credit card numbers, collection of SINs, procedures for shredding documents, drafting privacy policies, retention of client medical information, and applicable privacy laws. In addition, very few participants received training to help them deal with privacy issues on behalf of their company.

Business Challenges and Sources of Assistance

Economic issues are the top challenges facing small businesses and the sources they are most likely to turn to for advice or guidance are formal (e.g. company head office, professional or trade associations) and informal e.g. (peers, colleagues) networks.

Participants identified a variety of issues or challenges facing their businesses but the most frequently identified type of challenge tended to be economic, with a focus on competition, profitability, and growth/market share. A number of other challenges were identified, though none was identified by more than a few participants. According to participants, the issues and challenges facing their business tend to be the same or similar to those faced by their sector in general.

The most frequently identified source for advice or guidance on running their businesses were networks, both formal and informal. Such networks include colleagues, contacts and peers within their sector, a company's head office and internal sources/resources, suppliers, conferences, trade shows, professional or trade associations, and online sources. The only other sources identified with any frequency were lawyers and accountants.

Privacy Challenges Faced by Small Businesses

Most do not have experience addressing a customer's privacy-related concern. That said, there was unanimous agreement that protecting customers' personal information is an important issue, with most participants qualifying this as very important.

Most participants (a majority in each group) said their company has never been approached by customers with privacy-related concerns. Those who have been approached identified the following privacy-related questions, concerns, or requests: how personal information is managed and kept secure, why certain types of information are required, whether or not information is shared and if so with whom, why the customer was suddenly being contacted by other suppliers, requests that credit card information be destroyed after each transaction, concerns that information about criminal records will be shared with potential employers, and requests that the customer be allowed to provide requested information in-person rather than by email.

There was unanimous agreement that protecting customers' personal information is an important issue, with most participants qualifying this as *very* important. That being said, it does not tend to be a top-of-mind issue, concern, or preoccupation. By way of explanation participants routinely suggested that if reasonable measures/procedures are taken to protect customer information, the issue tends to remain a 'background' or 'back burner' issue. Not surprisingly, most participants (again, a majority in each group) said they have not formally assessed the privacy risks faced by their company or business. However, a caveat seems warranted in this regard as it is clear that many organizations consulted did take privacy-protective actions in order to mitigate risks to personal information they handle despite not undertaking formal assessments.

Approaches Used to Protect Customers' Information

Companies that collect customer information most often collect personal and financial information. To protect customers' information companies tend to use a collection of methods, including physical (e.g. locked cabinets, premises), technological (e.g. passwords, encryption), and organizational (e.g. restricting access to personal information to different levels of employees, shredding documents) measures. In addition, a few companies have privacy policies.

Personal information most often collected by companies about customers includes contact information (e.g. name, address, phone number, email address) and financial information (e.g. credit card number, bank account number, T4 data, salary). Contact information is typically collected to build relationships with customers and facilitate interaction with customers. Financial information is typically collected to facilitate transactions such as billing, crediting, pre-authorized payments, and tax-filing, but also for rental tenant reference checks. Some companies also collect biographical information (e.g. age, birthdate, gender, medical history, employment history). Reasons for collecting such information include rental tenant reference checks, meeting mandated/legal requirements, and to support provision of services (e.g. medical treatment, lawsuits).

Participants collectively identified a wide range of security measures designed to protect customers' personal information. These measures tend to fall into three categories: physical, technological, and organizational. The most frequently identified physical measures taken include locked cabinets, segregated zones/storage areas, alarm systems, and keypads/lock codes to access premises. The most frequently identified technological measures include password-protected computers/servers, encryption, firewalls, anti-virus software, and hard drive back-up. The most frequently identified organizational rules/procedures include limited/restricted access to files/storage rooms, non-disclosure/confidentiality agreements, not storing credit card numbers, shredding of documents, and scanning of documents. In addition to such practices a number of participants added that customer information is protected through good habits, vigilance, and common sense.

Despite having a range of security measures in place to protect customer information, the large majority of participants said that their company does not have a privacy policy. Companies that do have such a policy were more likely to be businesses with between 10-50 employees. Common reasons for having a privacy policy included the impression that it constitutes a good business practice and that it helps avoid potential problems or controversies. The main reason for not having a privacy policy was a perceived absence of need. Most often this was reflected in the observation that companies take reasonable measures and precautions to protect customer information, including reliance on professionalism and common sense. Consequently, there is no need to develop a formal privacy policy. Very few participants said that their companies communicate proactively with customers about their privacy practices, though some added that they would provide such information if asked by customers.

Compliance with Privacy Laws and Review of Information about PIPEDA

Very few participants are aware of the names of specific privacy laws that apply to their business. Most indicated that measures taken within their companies to protect customer information were motivated by 'common sense' or 'good business practice' and not by Canada's privacy laws.

Beyond a general awareness that such laws exist, very few participants are aware of the names of specific privacy laws that apply to their business. Underscoring the limited awareness of privacy laws, the large majority of participants indicated that they are unfamiliar with their responsibilities under such laws beyond a general awareness that they need to protect customers' personal information/maintain confidentiality. Only a few participants indicated that measures taken within their companies to protect customer information were taken in order to comply with Canada's privacy laws. Most indicated that measures were motivated by 'common sense', 'good business practice', 'protecting oneself', 'exercising due diligence', and 'a desire to maintain customer trust'.

Despite widespread lack of awareness of PIPEDA and limited familiarity with their responsibilities under Canada's privacy laws, participants routinely described the five principles (presented to them in a handout) as commonsensical or self-evident. Nor did participants have difficulty intuiting the meaning of the various principles, i.e., identifying what each one implies.

On the whole, participants' reaction to a document identifying the responsibilities of businesses for PIPEDA principles was positive. Participants routinely commented that

much or most of the information 'made sense to them', seemed 'logical' or 'self-evident', 'was not surprising', and 'included much of what they would have expected'. The document as a whole did not tend to elicit surprise or concern among participants. Information most likely to be described as new related to their responsibilities regarding giving customers access to their information.

Communications and Outreach

Few recalled receiving information about their company's privacy obligations. Organizations (e.g. professional associations), events/tools (e.g. webinars, trade shows), and various media (e.g. various social media, chat/support line) were suggested as ways for the OPC to reach businesses to raise awareness of their privacy obligations.

All but a few participants indicated that they have never received information about their company's privacy obligations. The Internet was most often identified as where they would go if they needed such information. Other frequently identified sources included peers, business associations, lawyers, accountants, and company head-offices. Governmental sources were identified relatively infrequently and included the Government of Canada, the Office of the Privacy Commissioner of Canada, Industry Canada, the RCMP, the Government of Ontario, and Service New Brunswick.

Participants collectively identified a number of ways the OPC could reach out to them to increase awareness about what they are required to do. These included organizations, events and tools, and various media. Information participants would like to receive from the OPC routinely included checklists of responsibilities/obligations and liabilities, updates/changes to the laws, suggestions/tips on best practices and how to protect information, and templates/models for developing privacy policies.

Messages most likely to motivate participants to pay attention to their company's privacy obligations tended to focus on the potential consequences of not doing so (e.g. potential liabilities, fines, loss of customers, and possible legal action). On the other hand, many felt that positive messaging would be as effective or more effective (e.g., "if you value your clients, protect their privacy").

More Information:
Supplier Name: Phoenix Strategic Perspectives Inc.
PWGSC Contract Number: 2R008-150157/001/CY
Award Date: 2015-11-10
Full Contract Amount: $103,998.42[1]
To obtain more information on this study, please email publications@priv.gc.ca.

[1] This report presents the results of the qualitative research. The results of the quantitative research are presented under separate cover.

Introduction

The Office of the Privacy Commissioner of Canada (OPC) commissioned Phoenix Strategic Perspectives Inc. (Phoenix) to conduct quantitative and qualitative opinion research with Canadian businesses on privacy-related issues. Phoenix is pleased to present the results of the qualitative research in this report.

Background and Objectives

The OPC is an advocate for the privacy rights of Canadians, with the powers to investigate complaints, conduct audits and publish information about the personal information-handling practices of public and private sector organizations. The OPC also conducts research and public education on privacy issues. Flowing from its mandate, the OPC is responsible for enforcing the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to commercial activities in the Atlantic provinces, Ontario, Manitoba, Saskatchewan and the Territories. Quebec, Alberta, and British Columbia each has its own law covering the private sector. Even in these provinces, however, PIPEDA continues to apply to the federally-regulated private sector and to personal information in interprovincial and international transactions.

Given the OPC's mandate to protect and promote privacy rights, and ultimately to provide guidance to individuals and organizations on privacy issues, it needs to understand the following with respect to Canadian businesses in their dealing with privacy issues:

- The extent to which businesses are familiar with privacy issues and requirements.
- The type of privacy policies and practices that businesses have in place.
- Businesses' compliance with privacy law.
- Businesses' awareness of emerging privacy issues and practices.

The OPC has regularly conducted quantitative surveys with businesses every two years. The research informs and guides the OPC's business outreach efforts.

The OPC recently identified new strategic priorities and approaches to help it achieve the goal of increasing Canadians' control over their personal information. In the summary report on the new priorities, *Mapping a Course for Greater Protection*, the OPC notes that, throughout stakeholder consultations, it heard that small and medium enterprises (SMEs) were in need of further outreach to reinforce their understanding of their privacy obligations under PIPEDA. As such, the Office seeks to deepen its understanding of small businesses, so that it can develop appropriate materials and approaches for enhancing its small businesses outreach.

Methodology

To meet the research objectives, quantitative and qualitative research were conducted with Canadian businesses. The focus of this report is the qualitative component of the study. For this component, a set of six groups was conducted between February 9th and 10th, 2016 with representatives of small businesses, with two groups in each of Toronto, Winnipeg, and Moncton. In each city, one group was conducted with representatives of businesses that employed fewer than 10 employees, and the other conducted with

representatives of businesses that employed 10 to 50 employees[2]. All companies had to collect personal information about their customers (e.g., customer names, telephone numbers, addresses, credit card numbers) to be eligible, and all participants had to deal to some extent with privacy-related matters for their company. The groups included a mix of businesses by sector, with up to half of the companies draw from the retail, legal, and residential real estate sectors. Recruitment was undertaken by Research House, under sub-contract to Phoenix, and participants received an honorarium of $250 in appreciation of their time.

In addition, the following specifications applied to the groups:

Groups with Under 10 Employees	Groups with 10 to 50 Employees
• Half the recruits had to be from businesses with fewer than five employees, and half from businesses with five or more employees. • There could be no more than two participants per group from single employee businesses. • There could be no more than two participants per group whose main responsibility is privacy and other compliance issues. • There could be no more than two companies per group engaged with privacy issues.[3]	• One-third each of the recruits were to be from businesses with 10 to 20 employees, 21 to 40 employees, and 41 to 50 employees.[4] • There could be no participants whose main responsibility is privacy and other compliance issues. • There could be no more than two companies per group engaged with privacy issues.[3]

The investigators for this study were Alethea Woods and Philippe Azzie. Philippe moderated the focus groups in Toronto and Moncton. Alethea moderated the groups in Winnipeg. Both moderators contributed to the final report.

Notes to Readers

- This research was qualitative in nature, not quantitative. As such, the results provide an indication of participants' views about the issues explored, but cannot be generalized to the full population of representatives of small businesses.

- In the course of exploring privacy-related issues with participants:
    - It became evident that many participants did not distinguish between protecting their customers' personal information and privacy, and protecting their clients' confidentiality and proprietary data. In other words, they did not distinguish between protection as it relates to business to consumer (B2C) activities, and protection as it relates to business to business (B2B) activities.

[2] Industry Canada defines a small business as anything under 100 employees. In order to ensure the groups were homogeneous enough to allow for full participation, the focus was narrowed to businesses with up to 50 employees. Companies with more than 50 employees are more likely to have a robust privacy structure and not the primary focus of the OPC's planned outreach.

[3] An 'engaged' company was defined as a company that has implemented 3 or more of the following measures: a) Identified someone responsible for dealing with privacy issues; b) Developed policies for staff that address privacy obligations; c) Put in place procedures for responding to customer requests for access to their personal information; d) Put in place procedures for dealing with complaints from customers who feel that their information has been handled improperly; e) Developed a privacy policy.

[4] This specification was relaxed in Moncton because of the limited number of firms with between 41-50 employees.

  - In some cases, participants explained situations involving the handling of health information which, in the provinces of New Brunswick and Ontario fall under the jurisdiction of substantially similar provincial legislation rather than PIPEDA.

- Appended to this report are the following materials: the recruitment screener, the moderator's guide, and the in-group materials distributed to participants.

Detailed Findings

Contextual Information

This section provides background information about participants with a focus on their role(s) within their respective companies with respect to privacy issues.

Main Responsibilities Within Company

Participants' main responsibilities within their companies varied. Groups included participants whose main roles involve the following:

- Responsibility for running the company in general (typically the owner of a company with fewer than 10 employees).
- Office management/administration/day-to-day operations, including bookkeeping, accounting, banking, equipment and material purchases, shipping and receiving.
- Sales and sales-related issues (including billing and other activities related to business to business transactions and business to customer transactions).
- Human resources, including hiring, training, and managing of staff.
- Client contact/interaction with clients, including booking appointments, initial client meetings/consultations, opening files for clients/collecting information (usually representatives of law firms and medical/dental clinics).
- Setting company policies and procedures, dealing with regulatory issues and compliance-related issue.
- Landlord-tenant-related activities, including screening potential tenants, having them fill out application forms, preparing leases/rental agreements.
- Fundraising for charities and surveying event attendees for charities.

Participants Are Responsible for a Range of Privacy-Related Issues

The types of privacy issues with which participants personally deal tend to fall into the following general categories, with participants sometimes having responsibilities in more than one area. Representatives of businesses with fewer than 10 employees were more likely to have responsibilities in more than one area.

- *Collecting information from customers*: This not only includes the initial collection of information but also keeping information up-to-date/updating information periodically or on an as-needed basis. It may also include obtaining consent from customers for the information collected and/or explaining why the information is being collected and how it will be used.

- *Managing the use, disclosure, and retention of information*: This can include ensuring proper storage/securing of collected information, managing/limiting access to information, determining how long to retain information and ensuring the information is retained for the required/stipulated length of time (and no longer).

- *Disposing of customer information*: This typically involves sending information for off-site storage and/or destruction of collected information (e.g. shredding), but it can include returning information to customers.

These responsibilities typically include ensuring compliance with company security practices/safeguards governing the collection, use, retention, and disposal of customer

information. Such practices are identified below in the section titled *Approaches Used to Protect Customers' Information*.

A few participants specified that they are responsible for drafting/developing the privacy policies/practices for their companies, including non-disclosure and confidentiality agreements with employees. These were more likely to be representatives of businesses with 10 employees or more.

Specific Tasks Associated with Privacy-Related Responsibilities

Specific tasks and activities participants undertake as part of their privacy role vary according to the aspect of customer-related information with which they tend to deal (i.e. collection of information, use/disclosure/retention of information, disposal of information). These tasks and activities are identified below and organized by the type(s) of issues with which participants deal.

Tasks related to collection of information

Specific tasks related to collecting information:

- Collecting/ensuring collection of required/needed information.
- Explaining to customers why information is required and how it will be used.
- Inputting customer information into the company computer system (e.g. data entry or scanning of paper documents containing customer information).
- Encrypting customer information.
- Creating back-up files of collected information.
- Updating customer information.

Tasks related to use, disclosure, and retention of information

Specific tasks related to use, disclosure, and retention of information:

- Filing/storing customer information according to company procedures.
- Limiting exposure of and access to customer information.
- Ensuring the confidentiality of client lists.
- Ensuring billing information/credit card information is properly secured.
- Having employees read/sign non-disclosure agreements.
- Ensuring information is retained for the required/mandated length of time.
- General monitoring of day-to-day security-related practices (e.g. making sure there are no open files on desks, making sure client business is not discussed publicly).

Tasks related to the disposal of information

Specific tasks related to the disposal of information:

- Returning information to customers.
- Sending information for shredding.
- Sending information for off-site storage.

Few Specific Difficulties Associated with Privacy-Roles

There was widespread agreement among participants that, on the whole, they have little difficulty completing tasks associated with their privacy role. That being said, some

participants did identify specific difficulties or challenges they face in this regard. None of these difficulties was identified by more than a few participants, however, and some were only mentioned by individual participants. Difficulties included the following:

- *Updating customer lists*: This was described as potentially challenging due to high turnover rates among customers.

- *Deciding how long to retain customer lists*: This was described as complicated due to the fact that relationships with customers may fluctuate (i.e. a company may lose and then regain a customer). This makes it difficult to determine how long customer lists should be retained (e.g. if a company loses a customer should it destroy that customer's information immediately or retain it in the hope that it can re-establish a relationship?).

- *Proper retention of customer information*: A few participants identified the issue of proper retention of customer information as potentially challenging due to the length of time it can sometimes take to settle an issue. This was a challenge faced by companies operating in specific sectors, such as the consulting and financial sectors. For example, tax appeals and legal cases may take a very long time to settle and during that time all client information must be protected and then retained for a mandated period of time (e.g. 10 years).

- *Preparing/drafting a company's privacy policy*: This was described as difficult to do without models or templates to follow because of lack of knowledge about what should be included in a company's privacy policy. This was more likely to be mentioned by those working for smaller companies, which do not have in-house resources to manage/advise on these operational considerations (as compared to those working for a company with multiple locations, including an administrative head office).

- *Coordinating information sharing between parties while maintaining confidentiality*: Sharing information between parties adds a dimension to the process of ensuring the confidentiality of information, which complicates it. The example given was a situation in which there is not a direct business-to-customer (B2C) relationship, but rather a business-to-customer relationship mediated by a business-to-business relationship (B2B). Concretely, this might be a financial advisor who works directly with customers, but needs to correspond with the Canada Revenue Agency on behalf of these customers (who are also clients of the Canada Revenue Agency). Multi-party relationships such as this one make the protection of information more challenging.

- *Balancing security with practicality*: This issue related specifically to keeping customer information encrypted. It was observed that there can be a temptation to delay the encryption of information until work on the file is complete rather than re-encrypting the information after each session of work. Put simply, if work on a customer file will take a week, it is less burdensome to encrypt the file once it is final rather than encrypting the product of each work session. This temptation has to be balanced against the need to secure customer information.

Limited Time Spent on Privacy Issues Compared to Other Job Responsibilities

The proportion of time typically devoted by participants to privacy issues tends to be quite limited. Asked to quantify this, a majority of participants estimated that it took up no more than five percent of their time. Most of those who said they devote more time to such issues estimated that it was in the range of five to 10 percent. Very few individuals said they spend more than 10 percent of their time on such issues.[5] Several landlords indicated that the time spent on such issues varies depending on the turnover rates in their rental units.

There were differences of opinion among participants as to whether it is easier or harder now to deal with privacy issues. Participants who felt it is easier now to deal with such issues gave the following reasons to explain why:

- The ability to collect information electronically makes it easier to collect and store (e.g. no need to scan documents, no need to shred documents).

- The greater importance devoted to security of customer information eliminates ambiguity related to the collection of such information. The basic rule is: *If you do not need it, do not collect it*. This makes things easier generally.

- The increased security measures in place and the greater attention devoted to this issue makes customers less reluctant about providing such information (i.e. it is easier to collect).

For their part, participants who felt it is harder now to deal with such issues gave the following reasons to explain their impression:

- The volume/amount of information collected and the ease in copying information (e.g. back-up files) makes it more of a challenge to ensure that information will be private.

- With the digitization of information, it is no longer possible to simply destroy customer information by shredding files. Back-ups, for example, cannot be as easily destroyed.

- Information is generally more difficult to collect now because customers fear possible breaches of security. This impression is clearly at odds with the impression identified above according to which customers are less reluctant to provide information.

Few Have Sought Advice to Help With Privacy Issues

Very few participants recall having looked for advice to help them with the privacy issues they deal with in their company. Those who have sought advice have done so in relation to specific issues, including questions related to the following: retention of credit card numbers, the collection of SINs, procedures for shredding documents, drafting a company's privacy policies, the retention of a client's medical information, and the privacy

[5] Only one person estimated devoting more than 50 percent of work time to privacy issues. In this case the individual explained that 50 percent was meant to express the significance the person assigns to ensuring the confidentiality of customers' information in day-to-day activities.

laws that apply to their company. Sources for such information included the company's head office, lawyers, accountants, 'Manitoba Health', 'Equifax' (a consumer credit company), 'Shred-it' (a company providing services related to destruction of information), and Internet searches. One participant could not recall where he/she looked for such advice. This small group of participants was mostly composed of representatives of businesses with 10 or more employees.

A few other participants specified that, while they have not looked for advice, they received unsolicited information related to privacy issues. This included information about the privacy laws that apply to their company, how to interface with PIPEDA, and assistance drafting a privacy policy. Sources for such information included an accounting firm and professional associations or governing bodies reaching out to members when the privacy laws were first implemented.

Very Few Have Received Training Related to Privacy Issues

Very few participants received training to help them deal with privacy issues. Such training as was received included a seminar offered by an accounting firm on how to coordinate and consolidate client information into one secure repository, a seminar on PIPEDA and CASL (Canada' anti-spam legislation), a workshop on the importance of maintaining privacy, and internal training on privacy issues as part of general orientation on protocols regarding accessing company systems and customer information. Individual participants identified each of these sources. Several other participants indicated that they received some 'informal' tips/suggestions regarding good practices related to privacy issues but no formal training.

Business Challenges and Sources of Help

This brief section reports on the main issues or challenges facing participants' businesses as a whole.

Main Business Challenges Facing Companies Tend to be Economic

Participants identified a variety of issues or challenges facing their businesses, but the most frequently identified type of challenge tended to be economic in nature. This included competition for customers and market share, company profitability, and company growth. Participants often referred specifically to their customer base, describing the main issue facing their company as 'shrinking markets', 'acquiring and retaining customers', and 'expanding their customer base'. Some described the main issue facing their firm as volatility in commodity prices and exchange rates, or more generally as the inability to forecast market conditions.

Other challenges also were identified, though none was identified by more than a few participants. These included:

- Digitalizing customer records.
- Constant learning (e.g. new software, new operating systems).
- Developing customer relations (e.g. building trust, meeting customer needs).
- Convincing customers of the safety of online payment transactions.
- Human resource issues (i.e. lack of skilled workers, accessing foreign workers).
- The length of time it takes to resolve the types of issues dealt with by the company (e.g. tax appeals, legal cases).
- Compliance with the standards of the payment card industry.
- Changes in practices/arrangements regarding funerals.
- The reluctance of prospective tenants to provide information.
- Getting clients to pay their bills.
- Getting information/intelligence about competitors.

It is worth noting that, although the challenges in this list may not be directly economic in nature, some of them can have an impact on a company's bottom line.

According to participants, the issues and challenges facing their business tend to be the same or similar to those faced by their sector in general.

Networks, Professional Associations – Main Sources for Guidance

The most frequently identified source for advice or guidance on running their businesses were networks, both formal and informal. When identifying such sources, participants routinely volunteered that they turned to them because they include people who experience similar challenges and who understand the issues the company faces. Such networks include colleagues, contacts and peers within their sector, a company's head office and internal sources/resources, suppliers, conferences, trade shows, professional or trade associations, and online sources (i.e. 'Meet-Up.com').

Specific professional or trade associations identified by participants included the following:

- Chamber of Commerce
- Manitoba Tourism Education Council

- Women's Entrepreneur Centre
- Manitoba Marketing Network
- Manitoba Rental Authority (Residential Tenancies Branch)
- Seed Winnipeg
- Real Estate Council of Ontario

The only other sources identified with any frequency were lawyers and accountants. A few participants mentioned government sources, but the only federal departments identified specifically by name were Immigration Canada, and Industry Canada.

Privacy Challenges Faced by Small Businesses

This section reports on privacy-related issues and challenges faced by small businesses.

Most Companies Have Not Been Approached by Customers with Privacy-Related Concerns

Most participants—a majority in each group—said their company has not been approached by customers with privacy-related concerns. A few participants were less categorical, specifying that they 'do not recall' their company ever having been approached by customers with privacy-related concerns.

On the other hand, at least a couple of participants in most groups reported that their company has been approached by customers with privacy-related questions or concerns. These included the following:

- Questions about how their personal information is managed and kept secure (e.g. credit card information, medical information).
- Questions about why certain types of personal information are required to complete the purchase.
- Questions about whether or not information is shared and if so with whom.
- Questions about why the customer was suddenly being contacted by other suppliers. (This occurred as a result of an employee selling customer lists to other suppliers).
- Requests that credit card information be destroyed after each transaction.
- Concerns that information about criminal records will be shared with potential employers.
- Request that the customer be allowed to provide requested information in-person rather than by email.

Participants who were contacted by clients all indicated that these matters were handled internally (i.e. with no external assistance).

Protecting Customer Information is Important but Not Top-of-Mind Concern

There was unanimous agreement that protecting customers' personal information is an important issue, with most participants qualifying this as *very* important. That being said, it does not tend to be a top-of-mind issue, concern, or preoccupation. By way of explanation participants routinely suggested that if reasonable measures/procedures are taken to protect customer information, the issue tends to remain a 'background' or 'back burner' issue. Some suggested that protecting customers' personal information is not a problem or issue until an issue or incident arises, and then it is dealt with. Still others said this is not something they think about a lot because of the limited amount of customer information they keep.

While not a major concern, a few participants explained that they sometimes wonder whether the measures in place to protect customer information within their business need to be improved or 'tightened-up'. A couple of participants said that protecting customers' personal information is something they do think about periodically because of the type of work they do (i.e. sharing information about tenants and being responsible for lists of donors to a charity).

Few Companies Reported Having Assessed Privacy Risks Related to Customer Information

Most participants—a majority in each group—said they have not assessed the privacy risks faced by their company or business. However, a caveat seems warranted in this regard. As has just been noted, participants routinely suggested that if reasonable measures are taken to protect customer information, the issue tends to remain a 'background' issue. Indeed, some reiterated this point to explain why their business has not assessed privacy risks (i.e. a risk assessment is not required if reasonable measures are in place). Moreover, as the examples of privacy practices identified in the next section reveal, businesses have taken a variety of measures to protect customer information. In other words, businesses have clearly implemented practices designed to address risks to the confidentiality of their customer information even though they may not have conducted a formal or explicit risk assessment.

Among those who indicated that their company ***has*** undertaken a risk assessment, a few described the assessment as 'informal' rather than 'formal'. They identified the following types of risks related to the personal customer information they collect and store:

- Employee theft (e.g. theft of client lists, intellectual property).
- Employee error/negligence (e.g. not shredding documents after scanning them, discussing client business in public places/areas, sharing information that should not be shared, leaving files unlocked, losing laptop computers, using weak passwords).
- Unethical cleaning staff (e.g. looking through desks after hours).
- Hacking (e.g. theft of billing information).
- Poor practices (e.g. copying/pasting information into emails).
- Customer error (e.g. leaving a completed application form in a public place/area).
- Lax or limited building security.

Approaches Used to Protect Customers' Information

This section reports on the type of personal information collected by companies and the approaches/processes in place within companies to protect such information.

Contact and Financial Information – Types of Information Most Often Collected

Types of personal information about customers most often collected by companies include basic contact information and financial information.

- *Contact information*: Contact information usually includes information such as name, address, phone number, and email address. This information is typically collected to build relationships with customers and facilitate transactions with customers. For example, such information is used to book appointments (e.g. dental or medical appointments), to inform customers that an order has arrived or that a shipment is being delivered/ready for delivery, and to allow businesses to contact customers regarding payment-related issues).

- *Financial information*: Financial information most often includes a credit card number. However, additional types of financial information collected include a bank account number, T4 data (including SIN), customer's federal tax ID number, salary, and credit/payment history. Financial information is typically collected to facilitate transactions such as billing, crediting accounts, monthly pre-authorized payments, and tax-filing. In the case of the federal tax ID number, the reason for collecting it is to facilitate cross-border shipping. Salary information is collected for tax-related reasons (i.e. by an accountant) and for proof of income (i.e. by a landlord). Credit history is also used by landlords to check a prospective tenant's credit rating before renting an apartment.

Some companies also collect biographical information. Such information may include age, birthdate, gender, information about family members/personal relations, medical history, employment history, purchase history, and criminal record. Such information is collected for a variety of reasons including rental tenant reference checks, meeting specific mandated/legal requirements, and to support the provision of services such as medical treatment, applications for immigration/work permits, and lawsuits/legal cases.

Types of information identified by individual participants include opinions/feedback from event attendees (collected in order to assess the event), information about clients' current natural resource mining activities/explorations (collected in order to assist the client with competitive intelligence), photographs (in order to facilitate a dental office's interactions with out of town clients), and information about times of the year when customers will not be at home (collected in order to ensure that orders will not be shipped during these periods).

Range of Measures in Place to Protect Customer Information

Participants collectively identified a wide range of security measures designed to protect customers' personal information. Moreover, most participants indicated that their company uses a variety of measures to protect customer information. These measures tend to fall into three categories: physical, technological, and organizational. Measures implemented

in each of these categories are identified below, with those identified most frequently preceded by an asterisk (*).

- Physical: These types of measures include the following:
  - *Locked cabinets
  - *Segregated zones/storage areas accessible only by pass key
  - *Alarm systems
  - *Keypads/lock codes to access premises
  - Video surveillance (identified only after prompting by the moderator)
  - Lock-boxes (Real estate)
  - Computers secured to desks

- Technological: These types of measures include the following:
  - *Password-protected computers/servers (i.e. customized logins)
  - *Encryption
  - *Firewalls
  - *Anti-virus software
  - *Hard drive back-up
  - Cloud computing security
  - Storage on protected/secure servers
  - Non-Internet enabled computers/servers for customer information
  - Restricted log-in access
  - Remote site back-up
  - Automated communications protocols (i.e. information sent directly to the clients as opposed to being copied and pasted into an email)

- Organizational: These types of measures include the following:
  - *Restricted access to files/storage rooms (e.g. through user authentication)
  - *Non-disclosure/confidentiality agreements with employees/customers
  - *Not storing credit card numbers
  - *Scanning of documents and destruction of hard copy versions
  - *Periodic shredding of documents
  - Periodic updating of passwords
  - Use of a safety impact checklist

In addition to those listed above, some informal practices are also implemented by many companies. These include the following:

- Informal training/briefing new employees on protecting client information
- Not leaving files on desk
- Not discussing clients in public areas of office

Finally, a number of participants specified that the main additional practices they have in place to protect customer information include good work habits, vigilance, and common sense.

Few Companies Have an Official Privacy Policy

Despite having a range of security measures in place to protect customer information, the large majority of participants said that their company does not have a privacy policy in

place. Companies that do have such a policy in place were more likely to be larger firms (i.e. those with between 10-50 employees).

Among participants' whose company developed a privacy policy, the most common reasons given to explain why included the impression that it constitutes a good business practice and that it helps avoid potential problems or controversies. A couple of participants explained that the decision was driven by the need to comply with regulations in their sector or that they were mandated to develop such a policy. One participant explained that the policy was developed in order to specify acceptable exceptions to the sharing of information with third parties.

Among participants' whose company has not developed a privacy policy, perceived absence of need was the main reason given to explain why. Most often this took the form of participants observing that their companies take reasonable measures and precautions to protect customer information, including reliance on professionalism and common sense. Consequently, there is no need to develop a formal privacy policy. Reasons provided by smaller numbers of participants to explain the lack of need for such a policy included the following:

- They are a small company and/or have no employees (one participant suggesting that if he/she had employees he/she would develop a privacy policy).
- The limited amount and nature of the customer information collected.
- They have never had a problem or encountered an issue that obliged their company to rethink their privacy practices and consider developing such a policy.

Beyond lack of need, the only reason given for not developing a privacy policy was not knowing/never being told that their company should have such a policy.

Features/Characteristics of Privacy Policies

Companies' privacy policies contained a variety elements or features, including the following:

- The type of information collected from clients.
- The reason for collecting types of information (i.e. how it will be used).
- How long collected information is retained.
- With whom such information will be shared.
- Acceptable exceptions to the sharing of information.
- How customers can have their information removed from company records.
- How to handle customers' questions about their personal information.
- How to safeguard customer information.
- Liabilities in case of security/privacy-related breaches.
- Contact information regarding customer held information.
- Rules regarding dissemination/discussion of customer information.

Some said their company received support in developing its privacy policy while others said they did not. Among those who said they received no assistance, a few added that they used a general template and adapted it or consulted the privacy policies of other companies. Those who did receive support identified the following sources for such support: BDO, their company Head Office, and the College of Dental Technologists.

Answers varied when participants whose companies have a privacy policy were asked how often their policy is reviewed. Answers ranged from 'yearly', to 'regularly' (undefined), to 'as-needed' to 'rarely/not often' to 'never'.

Asked finally whether the policy's goal is to inform customers or protect their business, participants whose companies have a privacy policy were most likely to emphasize the latter (i.e. protection) though a few emphasized both aspects.

Few Companies Communicate With Customers About Privacy Practices

Very few participants said that their companies communicate proactively with customers about their privacy practices, though some added that they would provide such information if asked by customers (i.e. 'on demand'). A few others observed that privacy-related information is included in contracts with customers (e.g. non-disclosure agreements) but not discussed explicitly. It was also observed that landlords will broach this topic informally by telling tenants what they can expect in terms of privacy.

The few who indicated that they do communicate with customers about their privacy practices specified that this is done when customers create an online account and approve/accept the 'terms and conditions' that regulate their interactions with the company. One participant specified that customers are asked to renew their approval of 'terms and conditions' once a year, which includes the company's privacy policies/practices.

Compliance with Privacy Laws

This section reports on issues related to the privacy laws that apply to businesses in Canada.

Limited Awareness of Applicable Privacy Laws

Beyond a general awareness that such laws exist, very few participants are aware of the names of any specific privacy laws that apply to their business. Only a few could identify either PIPEDA or the *Privacy Act* by name or knew the difference between the two. One participant specified that he is aware of PIPEDA because he took a course on how it applies to his work. Beyond PIPEDA and the *Privacy Act* the only pieces of legislation identified by name were CASL and Manitoba's *Health Information Protection Act* (HIPA), and each of these was identified by individual participants.

Limited Familiarity with Responsibilities Under Privacy Laws

Underscoring the limited awareness of privacy laws, the large majority of participants indicated that they are unfamiliar with their responsibilities under such laws beyond a general awareness that they need to protect customers' personal information/maintain confidentiality. Beyond this general awareness, the only specific responsibilities identified included the following, none of which was identified by more than a few participants.

- Get consent from customers for the information you are collecting.
- Explain to customers how the information collected will be used.
- Identify how long collected information will be retained.
- Explain with whom such information will be shared.
- Explain how such information will be protected.
- Do not share information with anyone other than those who have a right to see it.

The few participants who claimed to be at least somewhat familiar with their responsibilities under privacy laws tended to link this familiarity to the nature of their business and their job responsibilities. For example, one participant linked her familiarity with privacy laws to her work in the charities sector, explaining that under applicable privacy laws she cannot sell donor lists, must keep them secure, and must keep them up-to-date. Another participant linked his level of familiarity with such laws to the fact that he works in the area of information technology in the health sector.

Very Few Have Implemented Measures Specifically to Comply with PIPEDA

Only a few participants indicated that measures taken within their companies to protect customer information were taken, entirely or in part, in order to comply with PIPEDA and Canada's privacy laws. Among those who said their company made pointed efforts to comply, no one was under the impression that such compliance was difficult.

While some participants were unsure whether measures were taken in order to comply with PIPEDA, most indicated that measures were motivated by 'common sense', 'good business practice', 'protecting oneself', 'exercising due diligence', and 'a desire to maintain customer trust'. For reasons such as these, a number of participants volunteered that they assume their company is in compliance with applicable laws even though the measures in place were not taken in order to be compliant.

Review of Information about PIPEDA

At this point in the discussion, participants were successively given two handouts with information about PIPEDA. This section of the report describes participants' reaction to the information.

The first handout listed the names of five of the principles set out in PIPEDA to help businesses protect their customers' personal information. Participants were asked what they thought each principle meant.

Following this, participants were given the second handout. This one was more fulsome, identifying the responsibilities of businesses for each of the same five PIPEDA principles. Participants were asked to read the handout on their own in silence. As they were reading it, they were asked to circle anything that was new to them, as well as put a 'plus sign' beside anything their company currently does and a 'negative sign' beside anything that is a concern for their business or that they do not currently do.

Handout #1

a) Obtain valid, informed consent

b) Limit collection

c) Limit use, disclosure and retention

d) Use appropriate safeguards

e) Give individuals access

Handout #2

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada's federal private-sector privacy law. PIPEDA sets out the ground rules for how private-sector organizations collect, use or disclose personal information in the course of commercial activities across Canada. PIPEDA outlines 10 principles that businesses must follow. The following document outlines five of these principles, and some of the related responsibilities for each:

Obtain valid, informed consent

Your responsibilities

- Specify what personal information you are collecting and why, in a way that your customers can understand.
- Obtain the individual's consent before or at the time of collection, as well as when a new use of their personal information is identified. Consent is considered valid only if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure to which they are consenting.

How to fulfill these responsibilities

- Obtain informed consent from the individual whose personal information is collected, used or disclosed.

- Explain how the information will be used and with whom it will be shared.
- Retain proof that consent has been obtained.
- Do not deny a product or service to an individual who fails to consent to the collection, use or disclosure of information beyond that required to fulfill an explicitly specified and legitimate purpose.
- Ensure that employees collecting personal information are able to answer individuals' questions.

Limit collection

Your responsibilities

- Do not collect personal information indiscriminately.
- Do not deceive or mislead individuals about the reasons for collecting personal information.

How to fulfill these responsibilities

- Limit the amount and type of the information gathered to what is necessary for the identified purposes.
- Ensure that staff members can explain why the information is needed.

Limit use, disclosure and retention

Your responsibilities

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act.
- Keep personal information only as long as necessary to satisfy those purposes.
- Put guidelines in place for retaining and destroying personal information.
- Destroy, erase or render anonymous information that is no longer required for identified purposes.

How to fulfill these responsibilities

- Document and obtain consent for any new purpose for the use of personal information.
- Institute maximum and minimum retention periods that take into account any legal requirements or restrictions and redress mechanisms..
- Dispose of information that no longer fulfills its intended purpose in a way that prevents a privacy breach.

Use appropriate safeguards

Your responsibilities

- Protect personal information against loss, theft, unauthorized access, disclosure, copying, use or modification.

How to fulfill these responsibilities

- Develop and implement a security policy to protect personal information.
- Ensure security safeguards are reviewed and updated regularly.
- Use appropriate security safeguards to provide necessary protection.
- Ensure staff awareness by holding regular staff training on security safeguards.

Give individuals access

Your responsibilities

- When requested, inform individuals if you have any personal information about them.
- Explain how it is or has been used and provide a list of any organizations to which it has been disclosed.
- Give individuals access to their information.

How to fulfill these responsibilities

- Provide any help the individual needs to prepare a request for access to personal information.
- Respond to the request as quickly as possible, and no later than 30 days after receipt of the request.
- Make sure the requested information is understandable. Explain acronyms, abbreviations and codes.
- If information is amended by the individual, where appropriate, send new copies to any third parties that have access.
- If refusing to give access, inform individuals in writing, indicating the reasons and any recourse available.

PIPEDA Principles Resonate with Participants

Despite widespread lack of awareness of PIPEDA and limited familiarity with their company's responsibilities under Canada's privacy laws, participants routinely described the five principles as commonsensical or self-evident. While they may not have known them beforehand, they were not surprised or confused by them. Indeed, when reviewing the first handout (figure 1) some observed that they think their company's practices apply these principles even though the practices were not taken in order to comply with PIPEDA.

Participants Have no Difficulty Intuiting What Principles Mean/How They Apply

Participants had little to no difficulty intuiting the meaning of each PIPEDA principle, i.e., identifying what each one implies. Each of these principles is presented below, 'populated' with participant feedback about its specific meaning. As feedback tended to be similar across groups or represented variations on common themes, the focus is on conveying a sense of representative feedback rather than providing a full list of participants' actual verbatim comments.

Obtain valid, informed consent was seen to imply …

- Asking permission from the person from whom you are collecting information.
- Letting them know why you are asking for or need this information.
- Letting them know what you will be doing with the information you are collecting.
- Explaining what the person is committing to before collecting information.
- Making sure the person understands what you are asking.
- Ensuring the person has the right or is legally entitled to provide this information.
- Not exerting any pressure on the person (i.e. the information is provided willingly).

A question that emerged in the context of discussing this principle was whether or not 'valid, informed consent' implied written as opposed to verbal consent.

Limit collection was seen to imply …

- Collect only what you need.
- Collect minimal information.
- Collect only the essential.

Limit use, disclosure and retention was seen to imply …

- Protect the information collected against exposure.
- Only share information on a 'need-to-know' basis.
- Use information only in line with the reason for which it was collected.
- Make sure the appropriate employees have access; limit or restrict access.
- Don't sell what you collect.
- Don't keep information longer than necessary.
- Remove information when an active relationship with a customer ends.

Use appropriate safeguards was seen to imply …

- Set of measures taken to protect information.
- Secure information using whatever methods are needed.
- Develop best practices to safeguard information.
- Use means such as encryption, passwords, locked cabinets, shredding.
- Train staff.

Give individuals access was seen to imply …

- Individuals have a right to know what information you have collected about them.
- Disclose what is being collected.
- Keep clients informed of what you are doing with their personal information.
- Give people access to what is stored about them/allow them to see their files.

A question that emerged in the context of discussing this principle was the extent to which it requires companies to be proactive rather than reactive in terms of access (i.e. offering customers the opportunity to see/know about collected information vs. complying with customer requests in this regard).

Participants Aware of/Familiar with Most Responsibilities Associated with PIPEDA

Review of the second handout (figure 2) identifying responsibilities of businesses for each of the five PIPEDA principles elicited various responses. On the whole, participants' reaction was positive, in the sense that the content tended to be meaningful and familiar to them. For example, participants routinely commented that much or most of the information 'made sense to them', seemed 'logical' or 'self-evident', 'was not surprising', and 'included much of what they would have expected'.

The document as a whole did not tend to elicit any surprise or concern among participants. To the extent that anything was new to participants, it related to specific details. Participants were most likely to identify the following details as new information to them:

- Obtaining consent each time a new use of information is identified.
- Document and obtain consent for any new purpose for the use of personal information.
- Retain proof that consent has been obtained.
- Explain how information has been used and provide a list of any organizations to which it has been disclosed.
- Provide any help the individual needs to prepare a request for access to personal information.
- Respond to the request as quickly as possible, and no later than 30 days after receipt of the request.
- If information is amended by the individual, where appropriate, send new copies to any third parties that have access.
- If refusing to give access, inform individuals in writing, indicating the reasons and any recourse available.

As this list reveals, information most likely to be described as new to participants has to do with their responsibilities in relation to giving customers access to their information. This is not surprising, given that most participants indicated that their company has never been approached by any customers with privacy-related concerns.

Many also described the following information as new to them: *Do not deny a product or service to an individual who fails to consent to the collection, use or disclosure of information beyond that required to fulfill an explicitly specified and legitimate purpose*. However, in many cases participants described this information as new because it struck them as odd (i.e. they could not understand why a company or business would proceed in this way).

Some Responsibilities Elicit Questions

Some specific details in the second handout were identified as unclear or elicited questions from at least a few participants in most groups[6]. They included the following:

- What constitutes personal information (e.g. what is included and excluded from this category)?
- What is the Act? (This question seems to underscore lack of awareness of PIPEDA).
- What constitutes 'informed consent' (e.g. can it be implied, is verbal consent sufficient, must it be written)?
- What constitutes a 'new' use of customer information?
- What constitutes 'proof' that consent has been obtained (e.g. does this mean written consent is required)?
- What constitutes an 'indiscriminate' collection of information?

Companies Likely to Have Taken Measures Related to Variety of Principles

A majority of participants in each group indicated that their companies have taken at least some measures that comply with PIPEDA principles. Moreover, most indicated that their company has taken at least some measures in accordance with a number of these principles. Participants were most likely to acknowledge measures taken in relation to 'obtaining valid, informed consent', 'limiting the use, disclosure and retention of information' and 'using appropriate safeguards'. Companies were least likely to identify measures in place in order to give individuals access to their personal information. This is perhaps not surprising given that most participants indicated that their companies do not communicate with customers about their company's privacy practices.

[6] This is based on oral feedback from participants as well as review of their copies of the handout.

Communications and Outreach

This section reports on participants' feedback on issues related to communications and outreach.

Few Receive Information about Company's Privacy Obligations

Nearly all participants indicated that they have never received information about their company's privacy obligations. Among the very few who said they have received such information, one identified an information letter about the new privacy laws from the Government of Canada, one recalls a webinar that may have been given by a lawyer, and a couple cannot recall what they received (but were certain they had received something about their company's privacy obligations).

Internet – Most Likely Source for Information About Privacy Obligations

The Internet was most often identified by participants as where they would go if they needed information about their privacy obligations. They routinely specified that they would use the search term 'privacy laws' and specifications on this phrase (e.g. 'privacy laws in Canada'. Other frequently identified sources included peers, business associations, lawyers, accountants, and company head-offices. Lawyers, accountants, and company head-offices were most likely to be identified by companies with 10 or more employees.

Governmental sources were identified relatively infrequently and included the Government of Canada (unspecified), the Office of the Privacy Commissioner of Canada, Industry Canada, the RCMP, the Government of Ontario, and Service New Brunswick. Sources identified by individuals or no more than a few participants included human resources departments, BDO, banks, the Real Estate Council of Ontario, and Barreau du Nouveau Brunswick.

Variety of Ways the OPC Can Reach Out to Businesses

Participants collectively identified a number of ways the Office of the Privacy Commissioner of Canada could reach out to them and other businesses to increase awareness about what they are required to do. These included the following, organized thematically by channel/vehicle:

Organizations

- Canada Revenue Agency/CRA mailings (with HST forms)
- Business associations (e.g. Information Technology Association of Canada, Association of Professional Engineers & Geoscientists of Manitoba, Real Estate Council of Ontario).
- Banks
- Government of Canada (with specification that it look 'official' and/or be sent with government cheques)
- Canadian Federation of Independent Business
- Canadian Chamber of Commerce (and local Chambers)
- Canadian Manufacturers and Exporters
- Manitoba rental authority: Residential Tenancies Branch

- Lawyers/law firms
- Accountants/accounting firms

Events/Tools

- Webinars (accessible on demand and adapted by business size and sector)
- Seminars/workshops (in-person so as to facilitate Q&A sessions)
- Online training tool (accessible 24/7)
- Kiosks at trade shows/conferences

A few participants made a point of noting that they would prefer in-person seminars to online events such as webinars. They explained that while webinars which are accessible on demand allow participation at leisure, they are also easy to skip or miss. By comparison, they felt in-person meetings would make participants more accountable in terms of attendance. It was also observed by a few that exhibits or kiosks at events might not be very useful. The reason given was that individuals might be inclined to collect take-away resources made available by the OPC instead of engaging with its representatives (the latter being seen as a more fruitful exercise).

Media

- Newsletter (but only when there is important/new information)
- Pamphlets/posters
- YouTube videos
- Facebook
- Linked-in
- Ad campaign
- 1-800 phone number
- Chat line/support line

Few participants identified email as an effective way for the OPC to reach out to businesses. Many observed that they and their companies are swamped by emails on a daily basis and that an email message is likely to be ignored or pass unnoticed.

Types of Information Participants Would Like to Receive from the OPC

When it came to the type of information participants would like to receive from the Office of the Privacy Commissioner of Canada, the following were routinely identified:

- Checklists of responsibilities/obligations and liabilities (including an interactive tool that produces customized checklists of actions to be taken based on the type of information collected).
- Updates/changes to the laws.
- Suggestions/tips on best practices and how to protect information (adapted to various sectors).
- Templates/models for developing privacy policies.

The following were also identified, but less frequently:

- Online tests to assess knowledge/awareness regarding protecting information.

- Information about OPC audits/investigations (e.g. what is involved, how they proceed).
- Offer of a privacy protection assessment of firm conducted by the OPC.
- Information on how to assess the cost of compliance.

Some participants made a point of emphasizing that in order to be useful or effective, any information provided by the OPC should be targeted as much as possible by business size and sector.

Both Negative and Positive Message Considered Likely to Attract Attention

Messages identified as most likely to attract attention or motivate participants to pay attention to their company's privacy obligations tended to focus on the potential consequences of not doing so. This included potential liabilities, fines, loss of customers, and possible legal action. On the other hand, many felt that positive messaging focusing on the benefits of protecting client information would be as effective or more effective (e.g., "if you value your clients, protect their privacy"). A number of participants felt that both aspects (i.e., the positive and the potentially negative) should be emphasized, with a focus on protecting one's business and one's clients.

Effective messaging identified by small numbers included the possibility of mitigating the potential costs of compliance, the possibility of receiving some sort of OPC certification for compliance, and references to actual/concrete examples/cases to help emphasize the importance of protecting client information.

Some emphasized that whatever the messaging used, the message itself should be short and to-the-point. Focusing on style or approach, a few also suggested that messaging should include humour (e.g., "It's none of your business").

Appendix

Annex 1: Recruitment Screener

Specifications

- 2 groups per city:
  - Group 1: Under 10 employees
    - All companies must be privacy-relevant
    - Half the recruits to be from businesses with fewer than 5 employees
    - Half the recruits to be from businesses with 5 or more employees
    - Maximum of 2 recruits to be from single employee businesses
    - No participants who are unengaged from privacy issues
    - Maximum of 2 participants who are engaged with privacy issues
    - Maximum of 2 companies per group engaged with privacy issues
    - No participants who are lawyers
  - Group 2: 10 to 50 employees
    - All companies must be privacy-relevant
    - One-third to be from businesses with 10 to 20 employees
    - One-third to be from businesses with 21 to 40 employees
    - One-third to be from businesses with 41 to 50 employees
    - No participants who are unengaged from privacy issues
    - No participants who are wholly engaged with privacy issues
    - Maximum of 2 companies per group engaged with privacy issues
    - No participants who are lawyers
- Each group to be mixed by sector:
    - Half the recruits to be from targeted sectors:
      - Lessors of residential real estate
      - Retail
      - Legal
    - Half the recruitment to be from non-targeted sectors
    - No more than two recruits from any one sector
- Target individual: person most responsible for privacy related matters for company
- Recruit 8 for 5 to 6 to show
- Participants to be paid a $250 incentive

	Toronto (English)	**Moncton (French)**	**Winnipeg (English)**
	February 9	**February 10**	**February 10**
6:00 pm	<10 employees	10 or more employees	<10 employees
8:00 pm	10 or more employees	<10 employees	10 or more employees

Questionnaire

A. Introduction

Hello/Bonjour, 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." FOR FRENCH GROUP, IF PARTICIPANT WOULD PREFER TO CONTINUE IN ENGLISH, PLEASE RESPOND WITH, "Unfortunately, we are looking for people who speak French to participate in this discussion group. We thank you for your interest.]

I'm calling from Research House, a Canadian research firm. We're organizing a series of discussion groups on behalf of the Government of Canada to explore the needs and practices of businesses in relation to Canada's privacy laws.

May I speak to the person in your company who is the most familiar with the types of personal information collected about your customers and how this information is stored and used? This may be your company's Privacy Officer if you have one.

Yes	1	CONTINUE
No	2	THANK/TERMINATE

[INTERVIEWER NOTE: REPEAT INTRODUCTION WITH PRIVACY REPRESENTATIVE.]

Hello, my name is _____. I'm calling from Research House, a Canadian research firm. We're organizing a series of discussion groups on behalf of the Government of Canada to explore the needs and practices of businesses in relation to Canada's privacy laws. The groups will last up to two hours and people who take part will receive a cash honorarium to thank them for their time. May I ask you a few questions?

Yes	1	CONTINUE
No	2	THANK/TERMINATE

Participation is completely voluntary. We are interested in your opinions. No attempt will be made to sell you anything or change your point of view. The format is a "round table" discussion led by a research professional with up to eight participants. All opinions will remain anonymous and will be used for research purposes only in accordance with laws designed to protect your privacy.

[INTERVIEWER NOTE: IF ASKED ABOUT PRIVACY LAWS, SAY: "The information collected through the research is subject to the provisions of the *Privacy Act*, legislation of the Government of Canada, and to the provisions of relevant provincial privacy legislation."]

Before we invite you to attend, we need to ask you a few questions to ensure that we get a good mix of people in each of the discussion groups. This will take 5 minutes. May I continue?

Yes	1	CONTINUE
No	2	THANK/DISCONTINUE

[INTERVIEWER NOTE: IF INDIVIDUAL QUESTIONS THE VALIDITY OF THE RESEARCH, OFFER TO FAX/EMAIL HIM/HER THE VALIDATION LETTER. IF THIS DOES NOT SATISFY THE INDIVIDUAL, ASK HIM/HER TO CALL HEATHER ORMEROD OF THE OFFICE OF THE PRIVACY COMMISSIONER AT 819-994-5682 (OR HAVE HEATHER CALL THE RESPONDENT).]

B. Qualification

1. Does your company collect personal information about your customers? This includes things like customer names, telephone numbers or addresses, financial information like credit card numbers, and customer evaluations, opinions or feedback.

Yes	1	PRIVACY-RELEVANT
No	2	THANK/DISCONTINUE

2. How many full-time employees work for your company in Canada? Please include part-time employees as full-time equivalents. READ LIST. WATCH QUOTAS

One	1	GRP: UNDER 10
2-4	2	GRP: UNDER 10
5-9	3	GRP: UNDER 10
10-19	4	GRP: 10+
20-40	5	GRP: 10+
41-50	6	GRP: 10+
Over 50	7	THANK/DISCONTINUE

3. In which of the following sectors does your company operate? READ LIST. WATCH QUOTAS AND ENSURE GOOD MIX

Food services	1	TARGET SECTOR
Retail	2	TARGET SECTOR
Legal	3	TARGET SECTOR
Residential property management	4	TARGET SECTOR
Other. Specify: _____	5	NON-TARGET SECTOR

IF “3” AT Q3, ASK FOLLOW-UP:

4. Can you please tell me your position within your company?

Lawyer	1	THANK/DISCONTINUE
Legal assistant/paralegal	2	
Law clerk	3	
Office manager	4	
Administrative assistant	5	

CFO/financial manager	6
Owner/president	7
Other. Specify: _____	8

5. Which of the following statements best describes your role at your company with respect to privacy issues? READ LIST. WATCH QUOTAS: NO PARTICIPANTS WHO ARE 'UNENGAGED'; GRP: 10+ NO PARTICIPANTS WHO ARE 'ENGAGED'. GRP: UNDER 10 MAXIMUM OF TWO WHO ARE ENGAGED. GET GOOD MIX ACROSS OTHER CATEGORIES.

a) I NEVER deal with privacy-related matters, but I am the person most responsible for such issues.	1	UNENGAGED: THANK/DISCONTINUE
b) I RARELY deal with privacy-related matters, but I am the person most responsible for such issues.	2	
c) I SOMETIMES deal with privacy-related matters, but this is not my main responsibility.	3	
d) I OFTEN deal with privacy-related matters, but this is not my main responsibility.	4	
e) My main responsibility is privacy and other compliance issues.	5	ENGAGED: THANK/DISCONTINUE IF GRP: 10+

6. Which of the following has your company done? READ LIST. WATCH QUOTAS: MAXIMUM OF 2 'ENGAGED' COMPANIES PER GROUP.

a) Identified someone in your company who is responsible for dealing with privacy issues?	1	ENGAGED COMPANY IF 3+ ITEMS SELECTED BY RESPONDENT
b) Developed policies for staff that address your privacy obligations?	2	
c) Put in place procedures for responding to customer requests for access to their personal information?	3	
d) Put in place procedures for dealing with complaints from customers who feel that their information has been handled improperly?	4	
e) Developed a privacy policy?	5	

7. Have you, or your company, had any dealings with the Office of the Privacy Commissioner of Canada in the last 12 months?

Yes	1	THANK/DISCONTINUE
No	2	

8. Have you ever attended a discussion group or interview on any topic that was arranged in advance and for which you received money for your participation?

Yes	1	
No	2	SKIP NEXT QUESTION

9. When did you last attend one of these discussion groups or interviews?

Within the last 12 months	1	THANK/DISCONTINUE
Over 12 months ago	2	

10. Record gender by observation. TARGET GOOD MIX.

Female	1
Male	2

11. How comfortable are you with expressing your views in a group setting, including reading and commenting on written materials? READ OPTIONS

Very comfortable	1	
Somewhat comfortable	2	
Not very comfortable	3	THANK/DISCONTINUE
Not at all comfortable	4	THANK/DISCONTINUE

C. INVITATION TO PARTICIPATE

The group will take place on [DAY OF WEEK], [DATE], at [TIME]. It will last two hours. People who attend will receive $250 to thank them for their time and light refreshments will be served. Would you be willing to attend?

Yes	1	
No	2	THANK/DISCONTINUE

The discussion will be lead by a researcher from the national public opinion research firm, Phoenix SPI.

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 [INSERT FACILITY]. I would like to remind you that the group is at [TIME] on [DATE]. We ask that you arrive 15 minutes early.

At the facility, you will be asked to produce photo identification, so please remember to bring something with you (for example, a driver's license). If you use glasses to read, please remember to bring them with you. Participants may be asked to review some materials in [ENGLISH/FRENCH] during the discussion.

The session will be video recorded for research purposes and representatives of the Government of Canada research team will be observing from an adjoining room. You will be asked to sign a waiver to acknowledge that you will be video recorded during the

session. The recordings will be used only by the Phoenix SPI research team and will not be shared with others. As I mentioned, all information collected in the group discussion will remain anonymous and be used for research purposes only in accordance with laws designed to protect your privacy.

As we are only inviting a small number of people to attend, your participation is very important to us. If for some reason you are unable to attend, please call us so that we can get someone to replace you. You can reach us at [INSERT NUMBER] at our office. Please ask for [INSERT NAME].

Someone will call you the day before to remind you about the session.

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?

First name: _____
Last Name: _____
Email: _____
Daytime phone number: _____
Evening phone number: _____

Annex 2: Moderator's Guide

Introduction (5 minutes)

- Thank participants for attending
- Introduce moderator and Phoenix
- Tonight, we are conducting research on behalf of the Office of the Privacy Commissioner of Canada, or OPC, to discuss the needs and practices of businesses in relation to Canada's privacy laws.
- My job is to facilitate the discussion, keeping us on topic and on time.
- Your job is to offer your opinions about the issues to be covered tonight.
    - Not a knowledge test; no right or wrong answers (interested in opinions)
    - Looking for candour and honesty;
    - Okay to disagree; want people to speak up if hold different view
- Comments treated in confidence [MODERATOR: EMPHASIZE AS NEEDED BECAUSE THIS IS EXTREMELY IMPORTANT. THE OPC CAN INVESTIGATE COMPANIES AND THE CONCERN WAS RAISED BY SOME SURVEY PARTICIPANTS WHEN CONTACTED]; reporting in aggregate form only; recording for report writing purposes only; observers behind one-way glass.
- If you have a cell phone or other electronic device, please turn it off.
- Any questions?
- Roundtable introduction: Please tell us your first name, your position, and the sector your business is operating in.

MODERATOR: QUESTIONS WITH AN ASTERISK ARE TO BE ASKED ONLY IF TIME PERMITS.

Contextual Information (15 minutes)

When you were recruited for this study, all of you said you are the person who is the most familiar with the types of personal information collected about your customers and how this information is stored and used. Some of you might even be designated as the person responsible for dealing with privacy related matters on behalf of your company. I'd like to begin with a few background questions about your role in your company with respect to privacy issues.

1. What are your main responsibilities in your company? KEEP BRIEF

2. What types of privacy issues do you deal with when you think of the customers' information that you collect and hold? KEEP BRIEF

    Probe: - if needed:
    - questions and complaints from customers
    - investigations
    - oversight of security practices
    - requests from customers to see the personal information that your organization holds about them.

3. What kinds of tasks or activities do you do as part of your privacy role? Which, if any, of these things are difficult to complete? Why?

4. *What proportion of your time is spent on privacy issues compared to your other main job responsibilities? Is it harder or easier to deal with privacy issues now? Are there others in the company that deal with privacy? If so, what do they do?

   Probe: - relative importance of privacy function vs. other responsibilities

5. Have you ever looked for advice to help you with the privacy issues that you deal with at your company?

   Probe: - organizations used
   - tools/resources used
   - If INTERNET mentioned: ask about websites most visited/ bookmarked/trusted, go-to sources? [KEEP BRIEF]

6. Have you ever received training to help you deal with privacy issues? [GET HAND COUNT] If so, what did this look like—what was the nature of the training?

   *Probe: - exclusive focus on privacy vs. part of broader training
   - who provided it: company vs. external organization
   - needs met? Why/why not?

Business Issues/Challenges (10 minutes)

Thinking more broadly now and about your company as a whole,

7. What are the main issues or challenges facing your business? What about your sector as a whole? [KEEP BRIEF; FOCUS IS GENERAL, NOT PRIVACY SPECIFIC]

   Probe: - differences / similarities between business vs. sector

8. Who do you talk to, or where do you go, for advice or guidance on running your business? Why do you use these resources or supports? How helpful are they?

   Probe: - organizations used
   - tools/resources used (e.x., outsourcing services)

9. *Are these resources or supports enough for you? Do they meet your needs? If not, what's missing? What else do you need?

   Probe: - gaps

Privacy Issues/Challenges (15 minutes)

10. Thinking about your customers' personal information, how big of an issue is protecting this information to your business? Is this something you think about ever? What about your sector… how big of an issue is protecting customer information?

Probe: - level of perceived risk
- level of concern: do they think about it
- priority compared to other business issues/concerns
- differences / similarities between sector and business

11. Do you assess the privacy risks faced by your company or business? If so, what are the main privacy risks related to the personal information you collect and store about your customers?

Probe (as needed):
- employee theft, error
- lost USB sticks
- hackers/threat of data breaches/cyber-attacks
- security of 3rd party storage

12. *Are there other privacy issues faced by your business at this time?

Probe (as needed):
- proper use of video surveillance
- BYOD
- online privacy/e-commerce
- targeted advertising
- building customer profiles to provide more customized and personal service

13. Have customers ever approached your company with privacy-related concerns? If so, what were the concerns?

Probe: - type of concerns

14. How were these privacy-related concerns handled? Did you get any help in handling this? Who did you get it from?

Privacy Approaches/Processes (20 minutes)

I'd now like to discuss the handling of personal information and privacy matters by your company.

15. What type of personal information does your company collect about your customers and why?

Probe: - nature (e.g., contact information, financial information, opinions)

16. *How do you store this information? Anywhere else?

Probe: - paper, electronic formats
- online
- on-site, off-site (3rd party)

17. What does your company do to protect your customers' personal information?

Probe: - security measures in place
- regular risk assessments
- safeguards:
  - locked files, cabinets
  - building security
  - document shredding
  - password-protected computers
  - encryption

18. Beyond these measures to protect personal information, does your company have any other practices to help you protect your customers' personal information? This could be written procedures, informal practices that you regularly do, or training. [GET HAND COUNT] If not, why not?

    Probe: - formal versus informal

19. For those of you who said your company has practices in place:

    a. Let's focus first on informal practices. What does this look like…what types of things are included here (i.e., privacy related actions, activities, etc.)?
    b. What about formal procedures? What does this look like…what types of things are included here (i.e., privacy related actions, activities, etc.)?
    c. Did your company receive support to develop your practices and procedures? If so, who?
    d. Does your company provide staff with training about privacy obligations? If so, who can attend? How often is it offered? Who provides it?

    Probe: - for each one, probe for specific measures/actions

20. Does your company have a privacy policy? [GET HAND COUNT] If not, why not? If so, why did you develop it?

21. For those of you who said your company has a privacy policy: [KEEP BRIEF]

    a. What's in it?
    b. Did you receive any support developing it? If so, who provided it? What was it?
    c. How often do you review it?
    d. What's the policy's goal (to inform customers or protect your business?)

22. Do you communicate with customers about your company's privacy practices? If so, what do you tell customers about your practices? How (when and where?) do you tell them? How often…what triggers this?

    Probe: - changes in use
    - updates to policies

Compliance (35 minutes)

In Canada, both provincial and federal governments have privacy laws in place for businesses. I want to focus now on your company's responsibilities under relevant privacy legislation.

23. Are you aware of any privacy laws that apply to your business? If so, what are you aware of?

For those of you aware of privacy laws that affect your business,

24. How familiar are you with your responsibilities under privacy laws? What are your responsibilities?

25. *What don't you know about your responsibilities that you think you need to know more about?

The *Personal Information Protection and Electronic Documents Act*—commonly referred to as PIPEDA—is Canada's federal private sector privacy law. PIPEDA sets out rules for businesses to protect personal information.

26. Earlier in the discussion we talked about the different types of measures your company is taking to protect customers' information. Were any of these measures taken specifically to comply with PIPEDA and Canada's privacy laws? Was any of this difficult? If so, why?

    Probe: - note measures motivated by privacy laws
    - challenges / barriers experienced

27. *Did you receive any support? If so, who did you talk to, or where did you go, for advice or guidance?

We're now going to look at two handouts. Here's the first one. It lists the names of five of the principles set out in PIPEDA to help businesses like yours protect your customers' personal information. We're going to discuss each principle, one at a time DISTRIBUTE HANDOUT #1. GO THROUGH PRINCIPLES ONE SET AT A TIME.

Let's start with…..[ROTATE ACROSS GROUPS].

28. What do you think this means?

REPEAT FOR EACH PRINCIPLE.

Moving on. Here's the second handout. It identifies the responsibilities of businesses like yours for each of the same five PIPEDA principles. I'll give you a few minutes to read it. Please do this, on your own in silence, and we'll talk about it as a group when everyone is finished. When you are reading the document, please circle anything that is new to you, that you didn't know before. As well, please put a 'plus sign' beside anything your company currently does and a negative sign beside anything that is a concern for your business. Is this clear?

HANDOUT LIST. ALLOW PARTICIPANTS TIME TO REVIEW IT, AND THEN CONTINUE.

It looks like everyone has finished….

29. *First, what's your overall impression of what you just read? Why? Anything else?

    Probe: - positive/neutral/critical reaction

30. Overall, what did you learn that didn't know before? Anything else?

31. Before we continue, was there anything that was unclear in what you read?

Now I'd like to focus on each principle…Let's start with … [INSERT; ROTATE ACROSS GROUPS]. FOR EACH, ASK THE FOLLOWING QUESTIONS:

32. How, if at all, have you applied [would you apply] this principle in your business?
33. What did you find [do you think would be] most challenging?
34. What do you think would have helped [would help] you apply this principle?

REPEAT FOR EACH PRINCIPLE. *[If time is running short, do not explore Access principle]

Communications/Outreach (15 minutes)

Changing topics,

35. If you need information about your company's privacy obligations, where would you go?

    Probe: - channels, sources

36. Do you ever receive information about your company's privacy obligations? If so, from who? In what format? What type of privacy information is typically included in these materials? How useful is the information? What do you like about it, if anything?

    Probe: - industry associations
    - third-party professional services (lawyer, accountants, etc.)
    - email newsletter, email message, mail/paper

    Probe: - changes/updates to your obligations
    - legal interpretations of changes to obligations
    - helpful tips on how to comply

37. How can the Office of the Privacy Commissioner of Canada best reach out to you and other businesses like yours to increase awareness about what you are required to do?

    Probe: - channels: email, website

38. What type of information would you like to receive from the Office of the Privacy Commissioner of Canada?

Probe: - changes/updates to your obligations
- helpful tips on how to comply
- summaries of findings from investigations conducted by the Commissioner

39. What messages would attract your attention or motivate you to pay attention to your company's privacy obligations?

Probe: - consequences?
- benefits of complying?

*There are different ways that businesses could learn about their privacy obligations. Which, if any, of the following options do you think you would be of most interest to you? The first one is…[READ/ROTATE]:

A. An online training tool for small businesses that owners could use to learn about privacy or to train their staff.

B. Exhibits at events intended for small businesses. A booth or table at events with staff available to speak with small business owners face-to-face, answer questions, and distribute informational materials.

C. Presentations and webinars on privacy obligations for small businesses delivered in conjunction with events hosted by local chambers of commerce.

ASK Q40 AND Q41 AFTER EACH APPROACH:

40. *What do you think about that idea? What do you like about it? What do you not like about it?
41. *What would need to be done to maximize its effectiveness…ensure it meets your needs?

42. *Are there any other ways of communicating or tools for learning about privacy obligations that would be interest to a business like yours?

Conclusion (5 minutes)

43. *Any final thoughts or advice for the Office of the Privacy Commissioner of Canada as it works to provide guidance and information to businesses in relation to their privacy responsibilities?

Annex 3: Focus Group Handouts

Participant handout #1

a) **Obtain valid, informed consent**

b) **Limit collection**

c) **Limit use, disclosure and retention**

d) **Use appropriate safeguards**

e) **Give individuals access**

Participant Handout #2

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada's federal private-sector privacy law. PIPEDA sets out the ground rules for how private-sector organizations collect, use or disclose personal information in the course of commercial activities across Canada. PIPEDA outlines 10 principles that businesses must follow. The following document outlines five of these principles, and some of the related responsibilities for each:

Obtain valid, informed consent

Your responsibilities

- Specify what personal information you are collecting and why, in a way that your customers can understand.
- Obtain the individual's consent before or at the time of collection, as well as when a new use of their personal information is identified. Consent is considered valid only if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure to which they are consenting.

How to fulfill these responsibilities

- Obtain informed consent from the individual whose personal information is collected, used or disclosed.
- Explain how the information will be used and with whom it will be shared.
- Retain proof that consent has been obtained.
- Do not deny a product or service to an individual who fails to consent to the collection, use or disclosure of information beyond that required to fulfill an explicitly specified and legitimate purpose.
- Ensure that employees collecting personal information are able to answer individuals' questions.

Limit collection

Your responsibilities

- Do not collect personal information indiscriminately.
- Do not deceive or mislead individuals about the reasons for collecting personal information.

How to fulfill these responsibilities

- Limit the amount and type of the information gathered to what is necessary for the identified purposes.
- Ensure that staff members can explain why the information is needed.

Limit use, disclosure and retention

Your responsibilities

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act.