



## **FINAL REPORT**

### **Canadian Businesses and Privacy-Related Issues**

**Prepared for the Office of the Privacy Commissioner of Canada**

**December 2013**

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



**TABLE OF CONTENTS**

Executive Summary .....	i
Introduction .....	1
Collection and Storage of Personal Information.....	5
Personal Information Protection Practices .....	10
Privacy as Corporate Objective .....	17
Awareness and Impact of Privacy Laws .....	19
Compliance .....	22
Breaches .....	24
Corporate Innovation.....	29
Disclosures to Law Enforcement .....	34
Seeking Clarification About Responsibilities Under the Law .....	35
Office of the Privacy Commissioner of Canada.....	37
Corporate Profile .....	40
Appendix .....	41
Telephone Questionnaire .....	42

## EXECUTIVE SUMMARY

Phoenix SPI was commissioned by the Office of the Privacy Commissioner of Canada (OPC) to conduct quantitative research with Canadian businesses on privacy-related issues. The purpose was to better understand the extent to which businesses are familiar with privacy issues and requirements, and the types of privacy policies and practices that they have in place. A 15-minute telephone survey was administered to 1,006 companies across Canada, stratified by size of business. The results were weighted by size, sector and region using Statistics Canada data to ensure that they reflect the actual distribution of businesses in Canada. Data collection was conducted November 7-27, 2013. Based on a sample of this size, the results can be considered accurate to within  $\pm 3.1\%$ , 19 times out of 20. Results are compared to similar surveys conducted in 2007, 2010 and 2011. The 2013 survey includes modifications to the questionnaire to address the evolving privacy environment.

### Collection and Storage of Personal Information

Surveyed business representatives work for a mix of different companies in terms of the type of customers served. In total, 36% of these companies sell directly to consumers (i.e., members of the general public or some subset of it). Almost as many (35%) sell both to the general public and to other businesses/organizations. Approximately one-quarter (26%) sell only to other businesses/organizations.

In terms of the types of customer information collected, virtually all of the surveyed companies (97%) collect contact information, such as names, phone numbers, and addresses. The large majority (83%) collect location information, such as postal codes. Other types of information mentioned with some frequency include opinions, evaluations, and comments (27%), financial information, such as invoices credit cards, or banking records (25%), purchasing habits (18%), and medical information (13%). In terms of diversity of information collected, most companies (65%) collect either two (39%) or three (26%) different categories of information mentioned above. A quarter (24%) collect more than that, while 11% collect less.

Approximately two-thirds (68%) of Canadian businesses use customers' personal information to help provide service to those customers. Slightly less than one-third (31%) use it to build customer profiles. Also mentioned with some frequency are marketing (17%) and use for financial matters, such as accounting, billing and invoicing (14%).

Three methods are commonly used by Canadian businesses to store personal information about their customers, each identified by a clear majority of business representatives. These include paper records stored on site (62%), the use of on-site servers (58%), and the use of desktop computers (55%). No other methods came close. Nearly one-quarter (24%) use portable devices, such as laptops, USB sticks, or tablets, while smaller numbers use cloud computing (7%) or a third party (excluding cloud computing) (7%).

### Personal Information Protection Practices

Business executives whose firms use portable devices, such as laptops, USB sticks, or tablets, to store their customers' personal information were asked whether or not their company uses encryption to protect information stored in this way. In response, 36% said that they did, whereas 58% said they did not (6% were uncertain).

Canadian businesses use a number of methods to protect the personal information of their customers. More than three-quarters use technological tools, such as passwords,

encryption, or firewalls (78%), or physical measures, such as locked filing cabinets, restricting access, or security alarms (78%). Almost two-thirds (65%) use organizational controls, such as policies and procedures. Of those that use technological tools to protect customer information, almost everyone (98%) uses passwords. As well, 82% use firewalls, while 48% use encryption. Of businesses that use passwords, 55% have controls in place to ensure that employees use hard-to-guess passwords. Also, most require their employees to change their passwords: 21% require this monthly, 17% quarterly, 10% every six months, 10% yearly, and 6% less than this (27% do not require employees to change their passwords).

Business representatives were asked whether they had in place a series of mechanisms related to privacy practices. Four of the six privacy-related practices are used by half or more of surveyed businesses. This includes having a designated privacy officer (58%), having internal policies for staff that address privacy obligations (51%), having procedures for dealing with customer complaints (51%), and having procedures for responding to customer requests related to their personal information (50%). Fewer than half (45%) have a privacy policy that explains to customers how they collect/use customer personal information, while one-third regularly provide privacy training and education to staff.

#### Privacy as Corporate Objective

Most executives said their company attributes significant importance to privacy protection. More than half (59%) offered the highest score available (on a 7-point scale), indicating their belief that protecting their customers' personal information is an *extremely* important corporate objective. In total, 82% offered positive scores on the scale, indicating that this is an important objective. At the other end of the spectrum, only 7% indicated clearly that protecting customers' personal information was not an important objective for their firm.

Widespread confidence was expressed by business representatives in their firm's ability to fully protect the personal information they collect about their customers. More than two-thirds (69%) said they were *very* confident, while almost all of the rest (28%) expressed moderate confidence in this.

#### Awareness and Impact of Privacy Laws

Business executives were asked to rate their company's awareness of its responsibilities under Canada's privacy laws, using a 7-point scale (1 = not at all aware, 7 = extremely aware). Almost half (45%) think their firm is extremely aware of its responsibilities. In total, almost two-thirds (66%) offered positive scores above the mid-point on the scale, indicating a relatively high level of familiarity with their privacy responsibilities. At the other end of the spectrum, 20% offered scores below the mid-point of the scale, suggesting a relatively low level of awareness. Over time, companies' awareness of their responsibilities under Canada's privacy laws has been fairly stable since 2007 when tracking began.

Executives were also asked to rate their level of awareness of the *Personal Information Protection and Electronics Document Act* (PIPEDA), the federal private-sector privacy law, using the same 7-point scale. In this case, just over one-third (35%) were extremely aware of the legislation. In total, over half (57%) offered positive scores above the mid-point on the scale, once again indicating a relatively high level of familiarity with their responsibilities. However, 28% offered scores below the mid-point of the scale, suggesting that a significant portion of businesses still have a relatively low level of awareness of PIPEDA.

## Compliance

Business executives were asked how difficult it has been for their company to bring their personal information handling practices into compliance with Canada's privacy laws (using a 7-point scale: 1 = extremely easy, 7 = extremely difficult). The largest proportion (41%) were neutral, viewing this as neither easy nor difficult. Most of the rest (38%) rated compliance with Canada's privacy laws as easy, while 13% felt that this was difficult for their company. Over time, the perceived difficulty of bringing personal information handling practices into compliance with Canada's privacy laws has increased modestly, while the perception that it is very easy has decreased somewhat.

A lack of understanding of privacy legislation was identified most often (17%) as the most significant barrier or challenge in terms of complying with Canada's privacy laws. Eight percent or less cited a number of other barriers: staff/personnel time needed (8%), cost of compliance (other than staff) (7%), making sure employees comply (6%), the need to keep their knowledge up to date (5%), and keeping the information secure (4%). Fully 39% did not offer a response.

## Breaches

Surveyed executives were asked to rate their level of concern about a data breach, where the personal information of their customers is compromised (using a 7-point scale: 1 = not at all concerned; 7 = extremely concerned). Exactly half said they were not at all concerned about a data breach, while 24% said they were extremely concerned. In total, one-third offered scores above the mid-point of the scale, suggesting moderate concern about a data breach. Over time, Canadian businesses have become modestly less concerned about a data breach.

Executives were asked to identify what they think represents the greatest threat of a data breach occurring at their company. Heading the list were hacking (24%) and theft (19%). In addition, 11% identified employee error. A number of other potential threats were identified in small numbers (3% or less). Five percent of executives said they could think of no threats, while 25% did not provide a response.

Fifty eight percent of surveyed companies do not have guidelines in place in the event of a breach where the personal information of their customers is compromised and 5% were unsure. Conversely, 37% do have guidelines in place. The vast majority (95%) of businesses say they have never experienced a breach where the personal information of their customers was compromised. The proportion of companies who have guidelines in place to respond to a breach has increased modestly since 2011 (31%) and 2010 (34%)<sup>1</sup>. The number of companies (4%) who say they have actually experienced a data breach has remained virtually unchanged since 2011 and 2010 (3% each).

Representatives of companies that have experienced a breach were asked what steps their company took to address the situation. The most common response was notifying individuals who were affected (40%), followed by resolving the issue with the individual responsible for the breach (29%) and enhancing their security system (28%). As well, some companies issued training to their staff (18%), reviewed their privacy policy (18%), notified law enforcement (17%), notified the relevant government agencies (6%), took legal action (2%), obtained information from the government (1%), or notified relevant

---

<sup>1</sup> In 2013, the question wording was changed to ask about "any protocols or procedures in place" versus "any guidelines in place" in 2011 and 2010.

departments within the company (1%). Eight percent of companies pursued other means of addressing with the breach.

### Corporate Innovation

When asked whether their companies have policies in place to assess privacy risks related to their business, two-thirds (67%) said they do not, while 5% were uncertain.

Only 13% of surveyed businesses send customer's personal data to a third party for processing, storage or other services. Of this 13%, two-thirds (68%) claimed to be aware that when a company transfers personal information to a third party for processing, storage or other services, which can include the use of cloud computing, it remains accountable for that information. Conversely, 31% were not aware of this accountability.

In 2013, a larger proportion (13%) of companies used third parties for handling their customers' personal information than in 2011 (9%), however the proportion is still less than in 2010 (18%).<sup>2</sup> The number of companies with contracts in place to ensure their customers' information is protected by the third party has increased over time (59% vs. 54% in 2011 and 50% in 2010).

Business representatives were asked about their company's policy on allowing employees to use their personal electronic devices, such as smartphones, tablets or laptops, for work purposes. Approximately one in five (21%) companies allow employees to use their own devices for work. Of this 21%, two in three (64%) have not developed formal, internal policies to manage security issues related to employees using their own devices.

At this time, the vast majority of companies (96%) do not collect customers' personal information using apps on mobile devices, with only 3% of business representatives stating that their company does collect such data.

### Disclosures to Law Enforcement

Only a small number of companies (4%) say they have received requests from law enforcement representatives without a warrant for personal information in the last 2-3 years. Of those who have received such requests, 3% received a request between one and five times, and 1% received six requests or more. Approximately half (48%) of the companies who received the requests provided the information each time it was requested, while 40% never provided the information, and 13% provided the personal information "some of the time."

### Seeking Clarification About Responsibilities Under the Law

Most business representatives (86%) said their company has never sought clarification of its responsibilities under privacy laws in Canada. Approximately one in 10 companies have sought clarification.

For companies that have sought clarification, the Internet (43%) was the main information source. Following this, 19% have gone to government agencies (federal, provincial, or general), 14% have sought the advice of a lawyer, 12% consulted industry experts, consulting firms or education source, 9% asked an industry association, 9% contacted the privacy commissioner, and 4% used their company's internal resources.

---

<sup>2</sup> In 2010, the question asked only about using third party for information processing, whereas in 2011 it included processing, storage, or other services.

The proportion of companies (11%) that sought clarification on their responsibilities under Canada's privacy laws in 2013 is lower than in 2011 (13%), 2007 (22%) and 2010 (22%). Where executives go for clarification on privacy laws has changed substantially since tracking began in 2010. More executives (43%) now turn to the Internet for clarification than in 2011 (28%) and 2010 (18%); more also turn to industry experts, consulting firms and education sources (12% vs. 2% in 2010, but 16% in 2011).

#### Office of the Privacy Commissioner of Canada

Forty-one percent of surveyed executives said they were aware that the Office of the Privacy Commissioner of Canada has information and tools available to companies to help them comply with their privacy obligations.

Of executives who were aware of OPC resources, the majority (78%) report that they have never used them. Fewer than one in five (17%) report that they have used OPC resources, although 5% were uncertain. Among companies that have used OPC resources to comply with their privacy obligations, the OPC website (56%) was the main source of reference. As well, 23% used OPC policy guidance, 11% OPC publications, 4% an OPC exhibit or presentation, and 2% called the OPC Information Centre.

Executives were asked to rate the usefulness of privacy-related resources they received from the OPC (using a seven-point scale: 7 = extremely useful, 1 = not at all useful). Seventy-five percent rated their usefulness above the midpoint of the scale, with 35% stating that they were extremely useful. However, 21% reported their usefulness as neutral or lower. Five respondents offered low assessments of the usefulness of OPC resources (scores of 1-3) were asked why they found the resources or information not very useful. Reasons included that they already knew the information or that the information was not appropriate for their business size.

The perceived usefulness of OPC resources has increased since tracking began in 2010. Now, 75% feel OPC resources are useful (5 -7 on a 7-point scale), versus 72% in 2011 and 55% in 2010.

#### Privacy-Related Subgroup Differences

Firm size is the most apparent predictor of a company's attitudes toward privacy and the number of mechanisms they currently have in place to protect privacy. Larger companies (with at least 100 employees) are more likely to practice a variety of methods of protecting customers' information, to require employees to change their passwords routinely, to have designated representatives for privacy-related issues, and to have developed internal policies to address their privacy obligations. Larger companies are also more likely to place a higher amount of importance on protecting privacy, to have sought clarification of their responsibilities under privacy laws, and to have a higher awareness of PIPEDA. Companies with more employees are also more likely to seek clarification of their responsibilities under privacy laws.

When looking at the data by region, companies that are based in Quebec often provided responses that differed somewhat from businesses in the rest of Canada. For example, Quebec businesses are generally less likely to have procedures and mechanisms to protect personal information. Quebec-based businesses are also less likely to have appointed someone responsible for privacy issues and to have internal policies that address their privacy obligations. However, Quebec-based businesses are also least likely to collect customer information for providing services.



## INTRODUCTION

Phoenix Strategic Perspectives Inc. (Phoenix) was commissioned by the Office of the Privacy Commissioner of Canada (OPC) to conduct quantitative research with Canadian businesses on privacy-related issues.

### Background and Objectives

The OPC is an advocate for the privacy rights of Canadians with the powers to investigate complaints and conduct audits under two federal laws, publish information about personal information-handling practices in the public and private sectors, and conduct research into privacy issues. As part of this mandate, the OPC is responsible for overseeing compliance with 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, 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 extent to which Canadian businesses are familiar with privacy issues and requirements.
- The type of privacy policies and practices these businesses have in place.
- Businesses' understanding of Canada's privacy laws and their privacy responsibilities.
- Businesses' awareness of and responses to emerging privacy issues and practices.

The OPC seeks to understand these issues in the context of trends over time, through the tracking of key benchmarking questions. This research addresses these objectives and will be used to guide the OPC's approach to fulfilling its mandate with respect to Canadian businesses.

### Research Design

To meet the research objectives, a telephone survey was administered to 1,006 businesses across Canada.

The following specifications applied to the survey:

- The target respondent was a senior decision maker with responsibility and knowledge of their company's privacy and security practices.
- A stratified random sampling approach was used for the data collection. The sampling frame was purchased from Dun & Bradstreet (D&B). A random sample frame was generated based on a sample-to-completion ratio of 10:1 for each of the three target business size quotas: small (1-19 employees); medium (20-99 employees); and large (100+ employees). The sample frame was generated in proportion to business population by region within each of the three business size groups.
- A detailed interviewer briefing note was prepared by Phoenix (and approved by the OPC) to brief interviewers and guide the data collection process.

- A telephone pre-test was conducted in English and French, with 10 interviews in each official language. Interviews were digitally recorded for review afterwards.
- Upon completion of the pre-test, Phoenix listened to the interviews and reviewed the resulting data. The data collected during the pre-test was not included in the final survey dataset because changes were made to the questionnaire as a result.
- Interviews averaged 15 minutes and were conducted in the respondent's official language of choice.
- Calling was conducted at different times of the day and the week to maximize the opportunity to establish contact.
- Up to 10 call-backs were attempted to reach potential respondents before a sample record was retired.
- The sample was carefully monitored throughout the data collection period to ensure effective sample management to keep the study on target and maximize response rates.
- The survey was registered with Marketing Research and Intelligence Association's (MRIA) national survey registration system.
- Sponsorship of the study was revealed (i.e. OPC).
- Data collection was conducted November 7-27, 2013.
- The following table presents information about the final call dispositions for this survey, as well as the associated response rate (using the MRIA formula)<sup>3</sup>:

Call Disposition Table	
	Total
<b>Total Numbers Attempted</b>	<b>10,709</b>
<b>Out-of-scope - Invalid</b>	<b>1,124</b>
<b>Unresolved (U)</b>	<b>4,466</b>
<i>No answer/Answering machine</i>	4,466
<b>In-scope - Non-responding (IS)</b>	<b>1,623</b>
<i>Language barrier</i>	63
<i>Incapable of completing (ill/deceased)</i>	11
<i>Callback (Respondent not available)</i>	1,549
<b>Total Asked</b>	<b>3,496</b>
<i>Refusal</i>	2,293
<i>Termination</i>	50
<b>In-scope - Responding units (R)</b>	<b>1,153</b>
<i>Completed Interview</i>	1,006
<i>NQ - Quota Full - Company Size</i>	114
<i>NQ - Q1 (NOT FOR PROFIT/DK/REF)</i>	33
<b>Response Rate</b>	<b>15.9</b>

All work performed adhered to or surpassed industry standards as determined by the MRIA, the industry association for survey research, as well as applicable federal legislation (PIPEDA). In addition, all work was performed in accordance with the *Standards for the Conduct of Government of Canada Public Opinion Research – Telephone Surveys*.

## Analysis

Weights were applied to the final data to adjust for the sample design. Data was weighted to the national proportion of businesses to ensure representation by size, region and

<sup>3</sup> The response rate  $[R=R/(U+IS+R)]$  is calculated as the number of responding units [R] divided by the number of unresolved [U] numbers plus in-scope [IS] non-responding households and individuals plus responding units [R].

industry. Canadian statistics for the number of businesses by size, region and industry were obtained through the *Business Register* produced by Statistics Canada.

The weighting scheme was based on three variables: business size, region and industry. The Statistics Canada “Indeterminate” category of businesses was excluded from the business size distributions used to weight the survey data.

Three sets of weights were created for each of: 1) the overall results, 2) the regional results, and 3) the results by business size. The details are as follows:

- For the overall weight, results were first weighted by business size in each region. Three size breaks (1-9 employees, 20-99 employees and 100+ employees) and seven regions (British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, and the Atlantic provinces) were used. They were then weighted by industry on a national level using the North American Classification System (NAICS).
- For the regional results, a second weight was developed based on region (Newfoundland and Labrador, New Brunswick, Nova Scotia and Prince Edward Island, Quebec, Ontario, Manitoba, Saskatchewan, Alberta and British Columbia) and industry (again using the NAICS). As with the overall weight, the regional results were weighted at the national level only by industry.
- For the results by business size, a third weight was developed based on business size (1-9 employees, 20-99 employees and 100+ employees). As with the overall and regional weights, the results by business size were weighted at the national level only by industry using the NAICS.

### Notes to Readers

- Reference is made to findings from similar surveys conducted for the OPC with Canadian businesses in 2007, 2010 and 2011. Since weighting procedures and, in some cases, question wording differs among the surveys, comparisons over time should be interpreted with caution.
- All results in the report are expressed as a percentage, unless otherwise noted.
- Throughout the report, percentages may not always add to 100 due to rounding.
- Demographic and other subgroup differences are identified in the report. The text describing these differences throughout the report is **put in a box** for easy identification. Only subgroup differences that are statistically significant at the 95% confidence level or are part of pattern or trend are reported. The table on the next page details how characteristics have been grouped for the analysis.
- Appended to the report are copies of the questionnaire in English and French.

**Table 1: Subgroup Categories**

<b>Demographic Categories</b>	
<p><i>Core Industries<sup>4</sup>:</i></p> <ul style="list-style-type: none"> <li>◦ Accommodation and Food Services</li> <li>◦ Administrative &amp; Support, Waste Management and Remediation Services</li> <li>◦ Arts, Entertainment and Recreation</li> <li>◦ Educational Services</li> <li>◦ Finance and Insurance*</li> <li>◦ Health Care and Social Assistance</li> <li>◦ Information and Cultural Industries</li> <li>◦ Professional, Scientific, Technical Services</li> <li>◦ Public Administration</li> <li>◦ Real Estate and Rental and Leasing</li> <li>◦ Retail Trade</li> <li>◦ Transportation and Warehousing</li> <li>◦ Utilities</li> </ul> <p><i>Non-Core Industries:</i></p> <ul style="list-style-type: none"> <li>◦ Agriculture, Forestry, Fishing and Hunting</li> <li>◦ Construction</li> <li>◦ Management of Companies, Enterprises</li> <li>◦ Manufacturing</li> <li>◦ Mining and Oil and Gas Extraction</li> <li>◦ Other Services (except Public Admin.)</li> <li>◦ Wholesale Trade</li> <li>◦ Other</li> </ul> <p><i>Revenues</i></p> <ul style="list-style-type: none"> <li>◦ Less than \$1,000,000</li> <li>◦ \$1,000,000 to just under \$10,000,000</li> <li>◦ \$10,000,000 to just under \$20,000,000</li> <li>◦ More than \$20 million</li> </ul>	<p><i>Region:</i></p> <ul style="list-style-type: none"> <li>◦ Quebec</li> <li>◦ Atlantic Canada</li> <li>◦ Alberta</li> <li>◦ British Columbia (and the Yukon)</li> <li>◦ Greater Toronto Area (GTA)</li> <li>◦ Ontario (including GTA)</li> <li>◦ The Prairies (SK,MB) and NT, NU</li> </ul> <p><i>Company Business Model</i></p> <ul style="list-style-type: none"> <li>◦ Sells directly to consumers</li> <li>◦ Sells directly to other businesses/organizations</li> <li>◦ Sells directly to both consumers and other businesses/organizations</li> </ul> <p><i>Company Location:</i></p> <ul style="list-style-type: none"> <li>◦ Operates at this location only</li> <li>◦ Other locations, but only in province</li> <li>◦ Locations in other provinces, but only in Canada</li> <li>◦ Other locations, including outside Canada</li> </ul> <p><i>Business size:</i></p> <ul style="list-style-type: none"> <li>◦ Self-employed (1 employee)</li> <li>◦ 2-19 employees</li> <li>◦ 20-99</li> <li>◦ 100 or more employees</li> </ul>
<b>Attitudinal Categories</b>	
<ul style="list-style-type: none"> <li>• <i>Perceived Importance of Protecting Privacy</i> <ul style="list-style-type: none"> <li>◦ Unimportant (1-3)</li> <li>◦ Neither (4)</li> <li>◦ Important (5-7)</li> </ul> </li> <li>• <i>Awareness of Privacy Obligations</i> <ul style="list-style-type: none"> <li>◦ Unaware (1-3)</li> <li>◦ Neither (4)</li> <li>◦ Aware (5-7)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <i>Perceived Difficulty of Compliance:</i> <ul style="list-style-type: none"> <li>◦ Easy (1-3)</li> <li>◦ Neither (4)</li> <li>◦ Difficult (5-7)</li> </ul> </li> <li>• <i>Concern Over Data Breach</i> <ul style="list-style-type: none"> <li>◦ Unconcerned (1-3)</li> <li>◦ Neither (4)</li> <li>◦ Concerned (5-7)</li> </ul> </li> </ul>

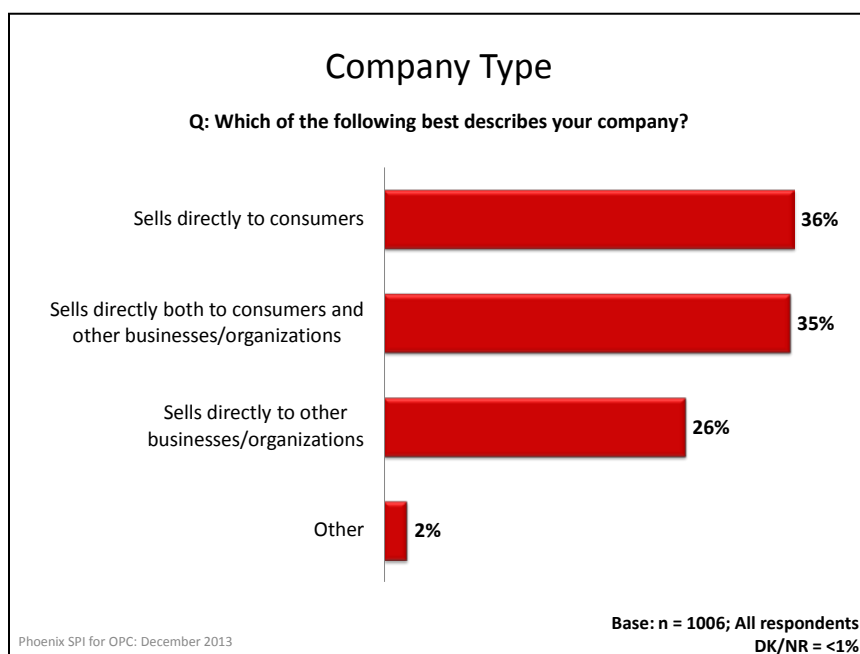
<sup>4</sup> The 'core' list of industries is an approximation that attempts to group industries that would be expected to collection customer personal information more than other industries (i.e. industries for whom privacy laws have greater relevance).

## COLLECTION AND STORAGE OF PERSONAL INFORMATION

This section identifies privacy-related practices adopted by businesses to protect customers' personal information. This includes the type of customers a business has, the type of information collected, how it is used, and the procedures and policies in place to protect this information.

### Different Company Types in Terms of Customers Served

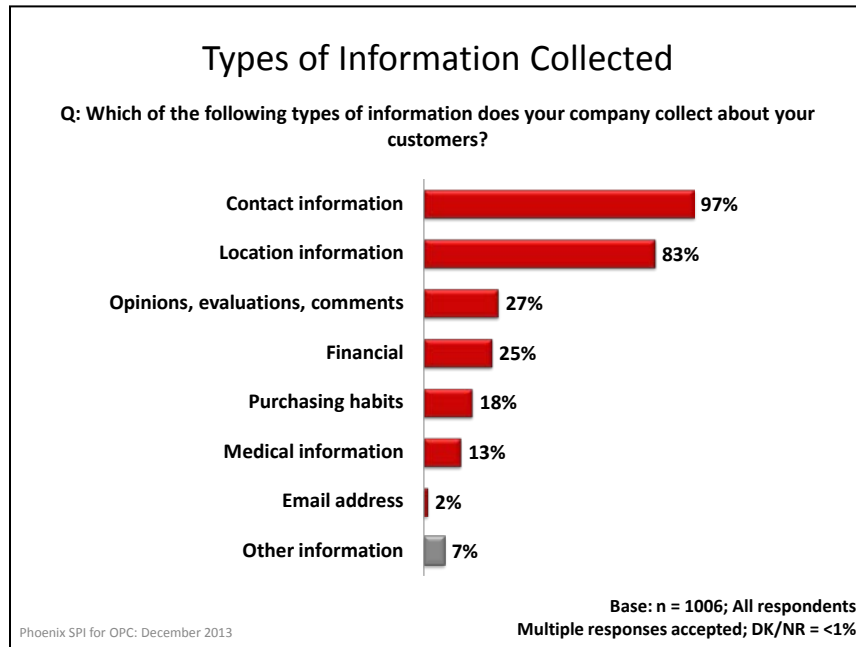
Surveyed business representatives work for a mix of different companies in terms of the type of customers served. In total, 36% of these companies sell directly to consumers (i.e., members of the general public or some subset of it). Almost as many (35%) sell both to the general public and to other businesses/organizations. Approximately one-quarter (26%) sell only to other businesses/organizations, while 2% provide services that do not fall into any of these categories.



### Contact, Location Information—Types of Information Widely Collected

In terms of the types of information collected about customers, virtually all of the surveyed companies (97%) collect contact information, such as names, phone numbers, and addresses. The large majority (83%) collect location information, such as postal codes. Other types of information mentioned with some frequency include opinions, evaluations, and comments (27%), financial information, such as invoices, credit cards, or banking records (25%), purchasing habits (18%), and medical information (13%). Two percent said they collect customer email addresses (undoubtedly others do also, but that is included in the 'contact information' category).

Information included in the 'other' category are birthdays, credit information, a Social Insurance Number, and a Driver's License number. In total, 1% said they do not collect any of these types of customer information.



In terms of diversity of information collected, most companies (65%) collect either two (39%) or three (26%) different categories of information mentioned above. Nearly a quarter (24%) collect more than that, while 11% collect less.

#### Subgroup Variations

The following subgroup differences were evident:

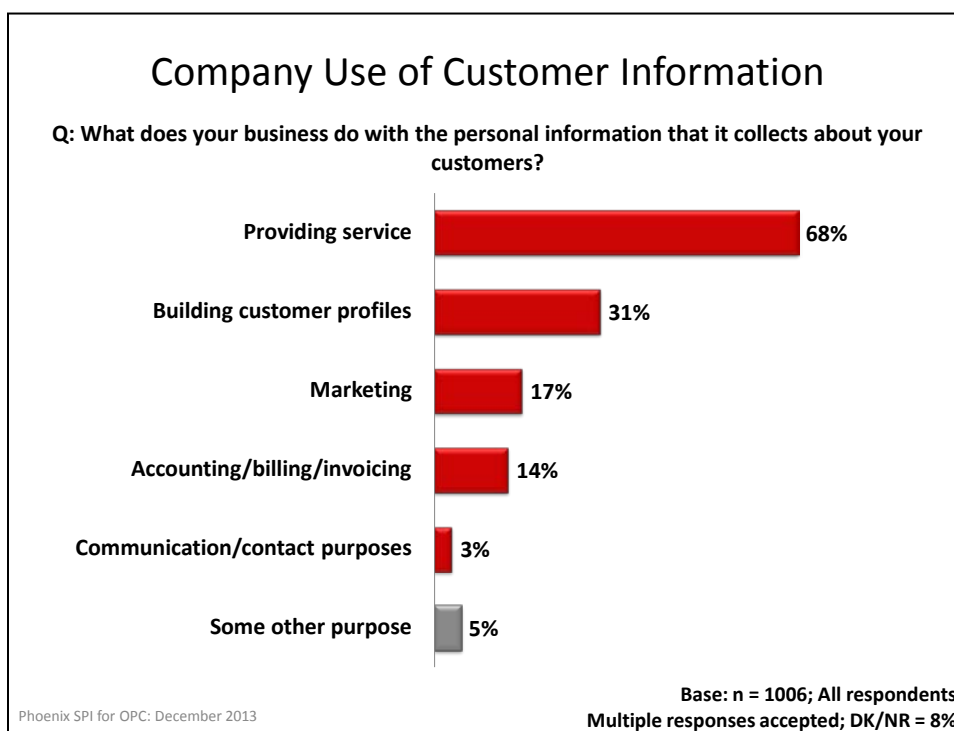
- Companies that sell *only* to consumers were generally less likely to collect customer data than companies that sell to businesses and companies that sell to both other businesses and consumers. For example, fewer companies that sell only to consumers collect location information (76%), financial information (19%), and information on purchasing habits (13%).
- Compared to smaller companies, larger ones generally collect more customer information. Companies with 100 employees or more (43%) are more likely to collect financial information than smaller companies: 37% of those with 20–99 employees, 24% of firms with 2–19 employees, and 14% of self-employed individuals. Larger companies are also more likely to collect the following information:
  - Customers' opinions, evaluations and comments (54%)
  - Customers' purchasing habits (29%)
  - Location information (90%)
  - Medical information (17%).
- Members of core industries are more likely than members in non-core industries to collect medical information (18% vs. 8% in non-core industries) and financial information (28% vs. 20% in non-core industries).
- Representatives of companies that attribute high importance to protecting privacy were more likely to report that their firm collects customers' opinions, evaluations and comments (30% vs. 6% of representatives that are neutral when it comes to protecting privacy and 12% of those that perceive it as unimportant), financial information (27% vs. 25% and 8% respectively) and medical information (16% vs. 1% and 3% respectively).

### Subgroup Variations (Cont'd)

- Representatives of companies with high awareness of their privacy obligations are most likely to work at a business that collects medical information from customers (18% vs. 6% of companies rated neutral on their awareness of their privacy obligations and 3% of companies reported to be unaware).
- Representatives who said their companies have had a hard time complying with Canada's privacy laws are most likely to work for firms that collect customers' opinions, evaluations and comments (37% vs. 26% of those who said it was neither difficult nor easy and 24% of those who saying it has been difficult).

### Providing Service—Most Common Use of Customer Information

Approximately two-thirds (68%) of Canadian businesses use customers' personal information to help provide service to those customers. Slightly less than one-third (31%) use it to build customer profiles. Other uses mentioned with some frequency are marketing (17%) and use for financial matters, such as accounting, billing and invoicing (14%). Only 3% identified using customer information for communications or contact purposes. Only 3% identified using customer information for communications or contact purposes.



**Subgroup Variations**

The following sub-group differences were evident:

- Quebec-based businesses (51%) are least likely to collect customer information for providing services, followed by Atlantic Canada (61%) vs. 73–80% of firms based elsewhere in Canada).
- Companies that sell *only* to consumers are least likely to use customer information for providing services and for accounting and billing purposes.
- Larger companies are more likely to use the customer data they collect for providing services (81% of those with 100+ employees vs. 70% or fewer of smaller companies) and building customer profiles to personalize services (41% of companies with 100+ employees vs. 28% of self-employed respondents).
- Businesses in non-core industries are more likely than core-industry businesses to use customer information for accounting and billing purposes (18% vs. 11% in core industries).
- Executives who are not concerned about a data breach are least likely to work for a company that uses customer information to build customer profiles to personalize their services (26% vs. 38% of those who are concerned and 43% of those who are neutral).
- Companies that have a privacy policy in place are more likely to use customer information for providing services (76% vs. 61% of companies with no official privacy policy) and for building customer profiles (36% vs. 27% of companies with no official privacy policy). Accordingly, representatives of companies without a privacy policy were more likely to choose “don’t know/no response” with respect to how their company uses customer information.

**Variety of Methods Used to Store Personal Information**

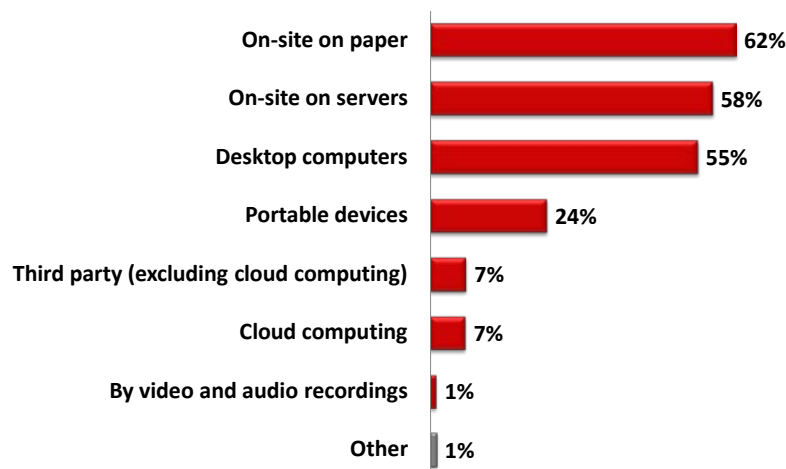
Three methods are commonly used by Canadian businesses to store personal information about their customers, each identified by a clear majority of business representatives. These include paper records stored on site (62%), the use of on-site servers (58%), and the use of desktop computers (55%). No other methods came close.

Nearly one quarter (24%) use portable devices, such as laptops, USB sticks, or tablets, while smaller numbers use cloud computing (7%) and a third party (excluding cloud computing) (7%).

Just over two-thirds (68%) of Canadian businesses use more than one method of storing the personal information they collect on their customers. Equal proportions (32%) of businesses use either one or two methods of storing customers’ information. Slightly more than one-third (36%) use three methods or more.

## Methods of Storing Personal Information

Q: In which of the following ways does your company store personal information on your customers?



Phoenix SPI for OPC: December 2013

Base: n = 1006; All respondents  
DK/NR = 3%

### Subgroup Variations

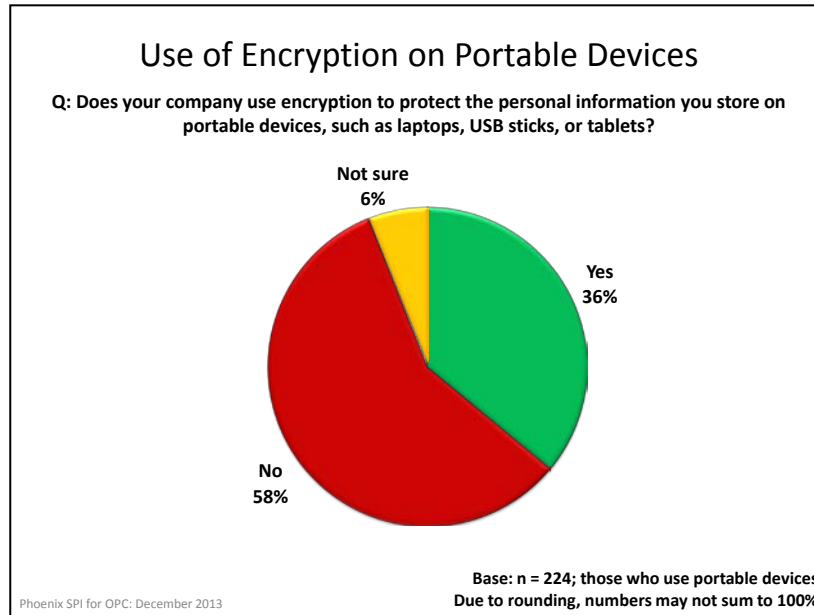
The following subgroup differences were evident:

- With respect to whether a company sells to consumers, businesses or both, companies that sell only to consumers are least likely to store customers' personal information on on-site servers (48% vs. 61 – 65% of other companies) and desktop computers (45% vs. 59 – 63% of other companies). Companies that sell only to businesses are more likely than other company types to store customer data on portable devices (32% vs. 18% and 23% of other companies).
- The likelihood of storing customer data on on-site servers increases with the size of the company. The largest companies (100+ employees) are also more likely to store customer data electronically through cloud computing. Smaller companies are more likely to store customer data on desktop computers.
- Companies in core industries are more likely to store customer data on on-site servers (61% vs. 53% of companies in non-core industries) and with a third party—excluding cloud computing—(10% vs. 3% for non-core industries).
- Companies that place a high degree of importance on protecting privacy are more likely to store customer data on on-site servers (60% vs. 53% of companies that perceive privacy as neither important nor unimportant and 44% that who view it as unimportant).
- Businesses that have a high awareness of their privacy obligations are more likely to store customer data on on-site servers than businesses with less awareness (62% vs. 53% of businesses neither aware nor unaware of their privacy obligations and 46% of those unaware).

## PERSONAL INFORMATION PROTECTION PRACTICES

### Minority Use Encryption on Portable Devices

Business executives whose firms use portable devices, such as laptops, USB sticks, or tablets, to store their customers' personal information were asked whether or not their company uses encryption to protect information stored in this way. In response, 36% said that they did, whereas 58% said they did not. Six percent were uncertain.



Compared to 2011, the number of businesses that store personal information on portable devices is virtually unchanged but the reported use of encryption on portable devices has decreased slightly: 36% vs. 44% in 2011.

### Subgroup Variations

The likelihood of using encryption was highest amongst companies that place a high degree of importance on protecting privacy (42% vs. 5% to 20% of companies that place lower degrees of importance on this) and companies that have a higher awareness of privacy obligations (49% vs. 11% to 19% of companies with lower awareness).

### Technological Tools, Physical Measures—Main Ways of Protecting Customer Information

Canadian businesses use a number of methods to protect the personal information of their customers. More than three-quarters use technological tools, such as passwords, encryption, or firewalls (78%), or physical measures, such as locked filing cabinets, restricting access, or security alarms (78%). Almost two-thirds (65%) use organizational controls, such as policies and procedures.

Seven percent said they take no measures.

Looked at somewhat differently, 77% of Canadian businesses use more than one method to protect the personal information of their customers. Conversely, 23% use only one.



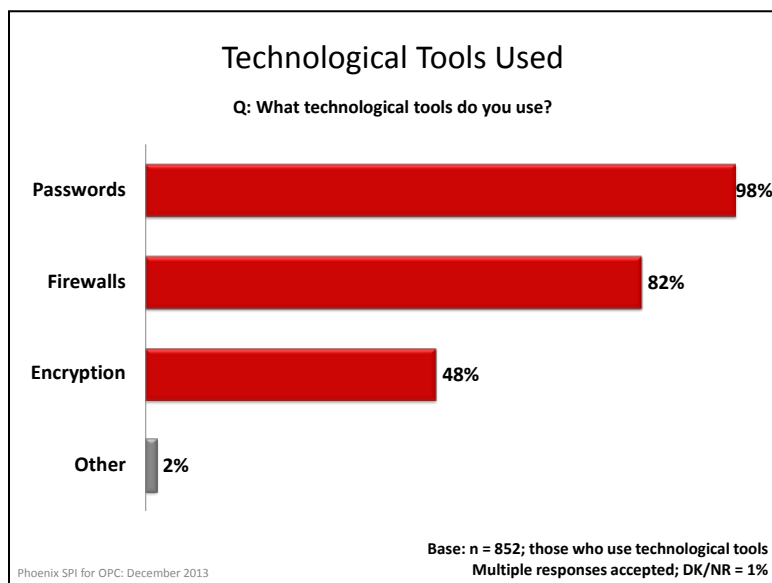
### Subgroup Variations

The following subgroup differences were evident:

- Companies in the Prairies are most likely (80%) to have policies and procedures (organizational controls) in place to protect customers' personal information, whereas Quebec-based companies (41%) are the least likely to have organizational controls in place.
- Companies that sell *only* to consumers are the least likely to use technological tools (66%) and specific organization controls (56%) to protect their customers' personal information. Businesses that sell to customers and businesses are the most likely to use physical measures such as locks and security alarms (84%).
- Larger companies are generally more likely to implement a variety of measures to protect their customers' information. Correspondingly, self-employed individuals are the most likely to have no measures in place to protect customers' information (24% vs. 1% to 5% of companies with two or more employees).
- Companies that perceive protecting privacy as unimportant are the least likely to implement security measures, such as using physical locks or security alarms (54%) and having privacy-related policies and procedures in place (33%). Conversely, companies that place higher importance on protecting privacy are the most likely to have implemented technological tools, such as passwords, encryption or firewalls (83%).
- Companies for which executives indicated awareness of their privacy obligations are less likely to have implemented technological tools (67%), physical controls (65%), and organizational controls (50%).

## Passwords, Firewalls—Most Common Tools Used to Protect Information

Of those that reported using technological tools to protect customer information, almost everyone (98%) uses passwords. As well, 82% use firewalls, while 48% use encryption.

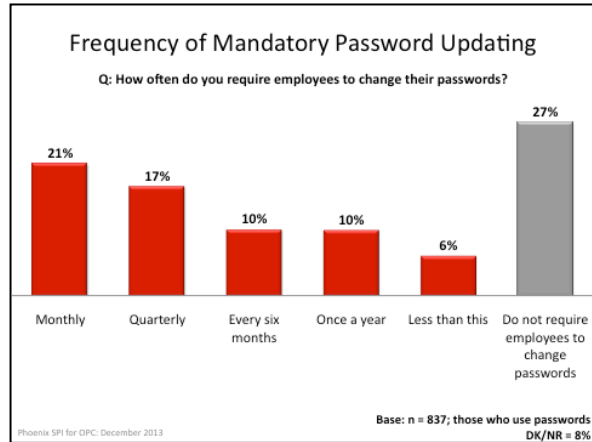
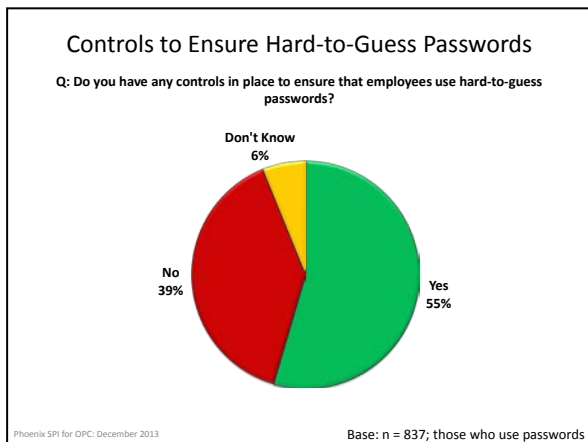


Compared to 2011, use of these tools has increased slightly: passwords (98% vs. 96% in 2011), firewalls (82% vs. 79% in 2011), and encryption (48% vs. 43% in 2011).

### Subgroup Variations

- The likelihood of using these technological tools was lowest among: companies in Quebec, self-employed individuals, and companies operating in non-core industries.
- Companies with 100 employees or more were the most likely to use all three tools.
- Businesses that reported they are highly aware of their privacy obligations were more likely to use all three tools.

Of businesses that use passwords, 55% have controls in place to ensure that employees use hard-to-guess passwords (6% were uncertain). Also, most require their employees to change their passwords: 21% require this monthly, 17% quarterly, 10% every six months, 10% yearly, and 6% less frequently than yearly. Just over one-quarter (27%) do not require their employees to change their passwords. These findings are virtually unchanged since the 2011 survey.



### Subgroup Variations

- A positive relationship was seen between how frequently companies require their employees to update their passwords and their perception of protecting privacy as important, and awareness of their privacy obligations.
- Companies with 100 employees or more expressed the most diligence in requiring employees to change their passwords—they were more likely to require employees to change their passwords monthly (29%) and quarterly (34%). Accordingly, companies with fewer than 100 employees were more likely not to have mandatory password changes (23% to 32% vs. 11% of companies with 100+ employees).
- A positive relationship was seen between the likelihood that a company has controls in place to ensure hard-to-guess passwords and: the perception they hold of the importance of protecting privacy, their awareness of their privacy obligations, and the perception of how difficult it is to comply with privacy laws.

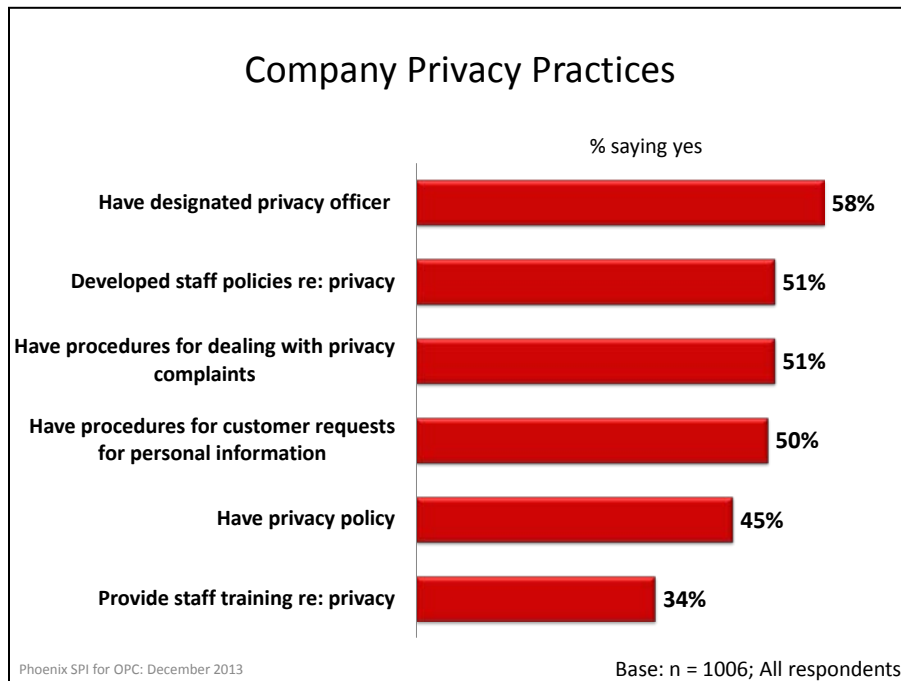
## Mixed Experience in Terms of Privacy Practices in Place

Business representatives were asked whether they had in place a series of mechanisms related to privacy practices. These mechanisms included:

- Having designated someone in their company to be responsible for privacy issues and personal information that the company holds
- Having documented internal policies for staff that address their privacy obligations under the law
- Having staff regularly receive privacy training and education
- Having procedures in place for responding to customer requests for access to their personal information
- Having procedures in place for dealing with complaints from customers who feel that their information has been handled improperly
- Having a privacy policy that explains to customers how they will collect and use customer personal information.

Four of these privacy-related practices are used by half or more of surveyed businesses. This includes having a designated privacy officer (58%), having internal policies for staff that address privacy obligations (51%), having procedures for dealing with customer complaints (51%), and having procedures for responding to customer requests related to their personal information (50%).

Fewer than half (45%) have a privacy policy that explains to customers how they will collect and use customer personal information, while one-third (34%) regularly provide privacy training and education to staff.



Approximately two in three (70%) firms have adopted more than one of these mechanisms. Two in five (40%) have adopted four mechanisms or more, 14% of firms employ only one mechanism, and 16% have not adopted any.

Number of mechanisms adopted	Percentage of firms	Percentage of firms with at least this many mechanisms adopted
None	16%	n/a
1	14%	84%
2	14%	70%
3	15%	55%
4	14%	40%
5	11%	26%
6	15%	15%

### Subgroup Variations

The following subgroup differences were evident:

- There was a positive relationship between **the likelihood of a company having designated someone to be responsible for privacy issues** and the following: the number of employees, their perception of the importance of privacy, and their awareness of their privacy obligations. The likelihood of having someone responsible for privacy issues was highest among:
  - Companies with 100 employees or more (72%)
  - Companies in core industries (62%)
  - Those who place a high importance on protecting privacy (64%)
  - Those most aware of their privacy obligations (65%).
- There was a positive relationship between the **likelihood of a company having developed internal policies that address their privacy obligations** and the following: the number of employees, their perception of the importance of privacy, and their awareness of their privacy obligations. The likelihood of having documented policies was highest among:
  - Companies with 100 employees or more (78%)
  - Companies in core industries (56%)
  - Those who place a high importance on protecting privacy (58%)
  - Those with more awareness of their privacy obligations (63%).
- There was a positive relationship between the **likelihood of a company providing their staff with privacy training and education** and the following: the level of importance they place on protecting privacy, their awareness of their privacy obligations, and their concern over a data breach. The likelihood of providing training was highest among the following:
  - Those who place a high amount of importance on privacy (39%)
  - Those with higher awareness of their privacy responsibilities (45%)
  - Those who are more concerned about a data breach (40%).
- The likelihood of **having procedures in place for responding to customer requests for information** was highest among the following:
  - Companies that sell to consumers and businesses (57%)
  - Companies in core industries (58%)



### Subgroup Variations (Cont'd.)

- Those that place a high importance on protecting privacy (57%)
- Those with higher awareness of their privacy obligations (57%).
- There was a positive relationship between the **likelihood that a company has procedures in place for dealing with complaints from customers who feel that their information was handled improperly** and the following: the number of employees, their perception of the importance of protecting privacy, their awareness of privacy guidelines, and their level of concern over a data breach. The likelihood of having procedures in place was highest among:
  - Companies that sell to businesses and consumers (58%)
  - Companies with 100 employees or more (61%)
  - Companies in core industries (55%)
  - Those that place a high amount of importance on protecting privacy (57%)
  - Those with higher awareness of their privacy obligations (59%)
  - Those with more concern about a data breach (55%).
- There was a positive relationship between **the likelihood that a company has a privacy policy that explains to customers how they collect and use the information** and the following: the number of employees, their perception of the importance of protecting privacy, and their awareness of their privacy obligations. The likelihood of having explanations for customers was highest among:
  - Companies with 100 employees or more (51%)
  - Companies in core industries (50%)
  - Those that place a higher level of importance on protecting privacy (51%)
  - Those with higher awareness of their privacy obligations (56%).

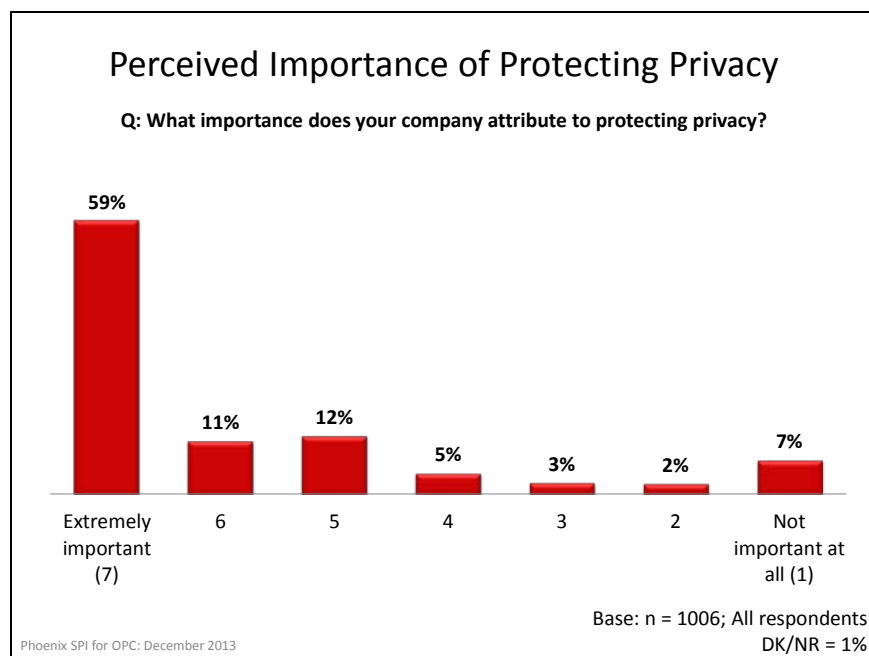
Companies in Quebec are generally less likely to have taken steps to improve their ability to privately manage customer information. For example, Quebec-based companies are less likely to have designated someone to be responsible for privacy issues and personal information (34% vs. 55% to 67% of firms in other regions) and to have a privacy policy that explains to customers how they collect and use their personal information (24% vs. 46% to 58% of firms in other regions).

## PRIVACY AS CORPORATE OBJECTIVE

This section explores perceptions of privacy as a corporate objective, and confidence in their firm's ability to protect customers' personal information.

### Most Attribute Significant Importance to Protecting Privacy

Most business executives said their company attributes significant importance to privacy protection. More than half (59%) offered the highest score available (on a 7-point scale), indicating their belief that protecting their customers' personal information is an extremely important corporate objective. In total, 82% offered positive scores on the scale, indicating that this is an important objective. At the other end of the spectrum, 7% indicated clearly that protecting customers' personal information was not an important objective at all for their company.



### Subgroup Variations

The likelihood of placing a high amount of importance (6 or 7 on a 7-point scale) on protecting privacy was highest among:

- Companies that sell to consumers only (65%) or that sell to consumers and businesses (62%) vs. 44% of those that sell only to businesses
- Companies with 100 employees or more (67% vs. 55% and 59% of small- and medium-sized companies)
- Companies in core industries (65% vs. 50% of others)
- Those with a higher awareness of their privacy obligations (85% vs. 54% or fewer of companies with lower levels of awareness)
- Those with higher concerns over a data breach (70% vs. 52% to 58% of companies that are not concerned about a data breach).



## Widespread Confidence in Firm's Ability to Protect Information

There was widespread confidence expressed by business representatives in their firms' ability to fully protect the personal information they collect about customers. More than two-thirds (69%) said they were very confident, while almost all of the rest (28%) expressed moderate confidence in this.



## Subgroup Variations

The following subgroup differences were evident:

- Executives at companies that sell only to consumers were more confident in their company's ability to protect customer information (73% vs. 61% of companies that sell to businesses and 68% of companies that sell to consumers and businesses).
- Confidence was higher among companies operating in core industries (72% vs. 65% of others).
- Those who perceived protecting privacy as important had more confidence in their firm's ability to protect customers' information (74% vs. 28% of companies that are neutral on protecting privacy and 53% of those that view it as unimportant).
- Those who perceive their company's awareness of their privacy obligations as high had more confidence in its ability to protect customer information (77% vs. 61% or fewer of companies with lower reported levels of awareness)
- Those who perceived it to be easy to comply with privacy laws had more confidence in their company's ability to protect customers' information (79% vs. 66% or fewer of companies that do not find it easy)

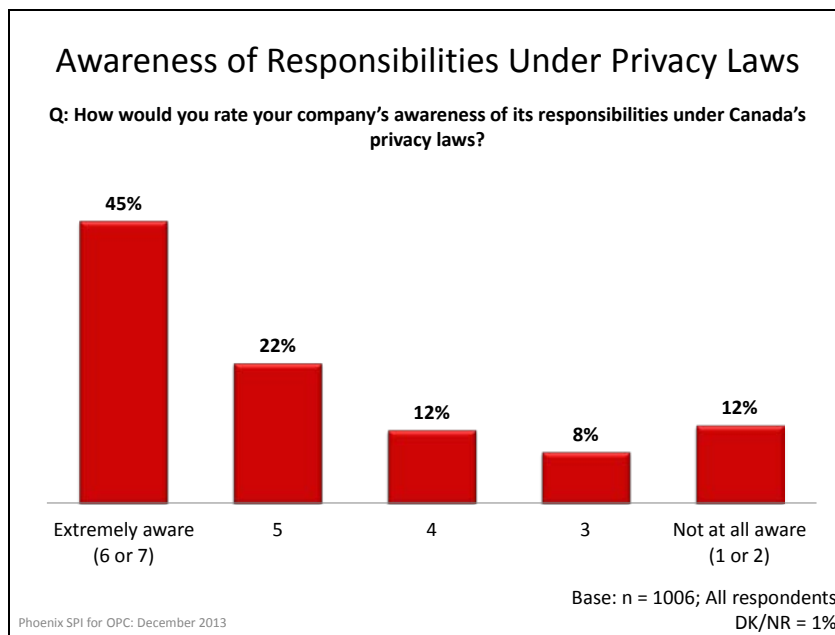
## AWARENESS AND IMPACT OF PRIVACY LAWS

This section explores executives' awareness of privacy laws in Canada. Questions in this section were prefaced with the following description of Canada's privacy laws:

*The federal government's privacy law, the Personal Information and Protection and Electronic Documents Act or PIPEDA, sets out rules that govern how businesses engaged in commercial activities should protect personal information. In Alberta, BC and Quebec, the private sector is governed by provincial laws, which are considered to be similar to the federal law.*

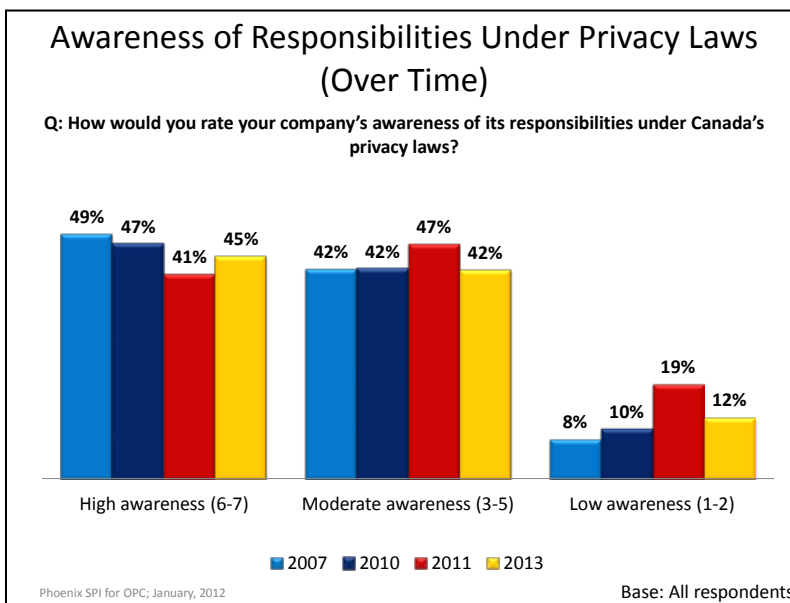
### Increasing Awareness of Company's Responsibilities Under Canada's Privacy Laws

Business executives were asked to rate their company's awareness of its responsibilities under Canada's privacy laws, using a 7-point scale (1 = not at all aware, 7 = extremely aware). Almost half (45%) think their firm is extremely aware of its responsibilities, while an additional 22% claimed some level of awareness (score of 5). In total, two-thirds (67%) offered positive scores above the mid-point on the scale, indicating a relatively high level of familiarity with their privacy responsibilities.



At the other end of the spectrum, 20% offered scores below the mid-point of the scale, suggesting a relatively low level of awareness.

Over time, companies' awareness of their responsibilities under Canada's privacy laws has been fairly stable. The proportion of companies with a high awareness of their privacy responsibilities has decreased only slightly, from 49% in 2007 to 45% in 2013. The percentage of companies with moderate awareness has remained unchanged at 42%, with just a single increase to 47% in 2011. In total, 12% express a low awareness of Canada's privacy laws, down from 19% in 2011, and up from 8% in 2007 when tracking began.



### Subgroup Variations

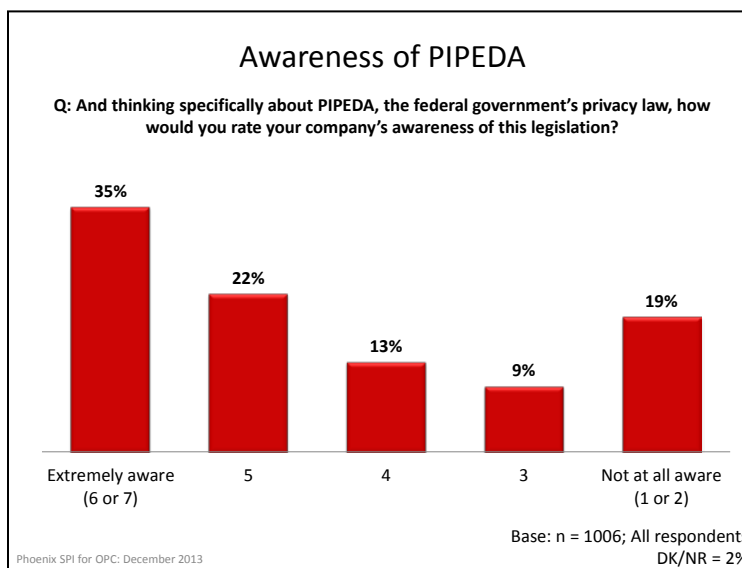
The likelihood of reporting high (6-7) awareness of responsibilities under Canada's privacy laws was highest amongst:

- Companies that sell only to consumers (49% vs. 44% of other companies that sell to consumers and businesses and 38% of companies selling only to businesses)
- Companies with 100 employees or more (65% vs. 41% and 46% of small- and medium-sized companies)
- Those who view protecting privacy as important (51% vs. 17% or fewer of companies that do not view protecting privacy as important)
- Those most concerned about a data breach (54% vs. 40% or fewer of representatives who are neutral or unconcerned).

### More Limited Awareness of PIPEDA

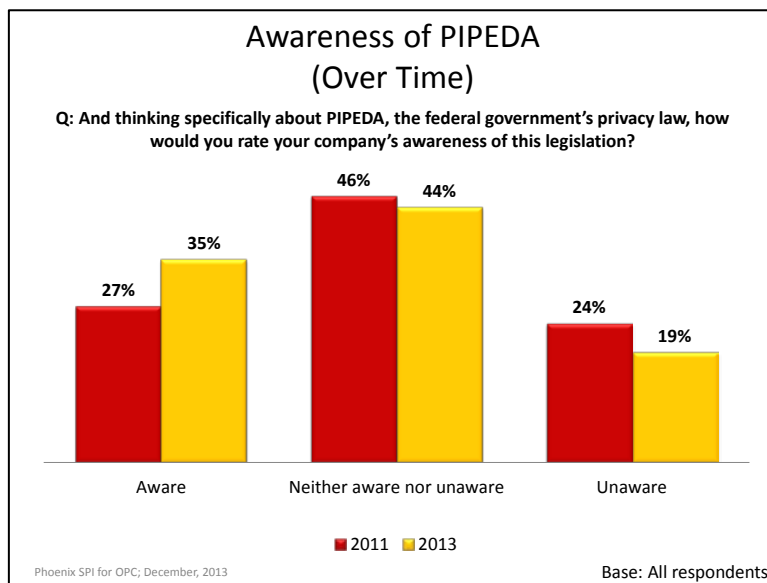
Executives were also asked to rate their level of awareness of PIPEDA using the same 7-point scale. In this case, just over one-third (35%) were extremely aware of the legislation, while 22% expressed some awareness (score of 5). In total, therefore, over half (57%) offered positive scores above the mid-point on the scale, once again indicating a relatively high level of familiarity with their responsibilities.

However, 28% offered scores



below the mid-point of the scale, suggesting a relatively low level of awareness. Awareness of PIPEDA specifically is therefore slightly lower than awareness of responsibilities under Canada's privacy laws more generally.

Businesses' awareness of PIPEDA increased modestly, from 27% in 2011 to 35% in 2013. Accordingly, the number of executives reporting that their company is unaware of this legislation decreased slightly (from 24% in 2011 to 19% in 2013).



### Subgroup Variations

The likelihood of reporting their company's awareness of responsibilities under Canada's privacy laws as very high (6-7) was highest amongst:

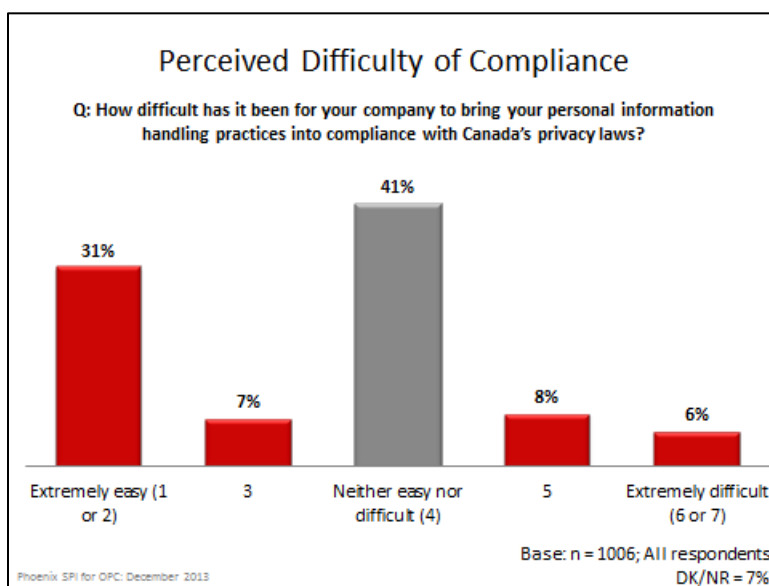
- Companies with 100 employees or more (54%)
- Companies in core industries (38% vs. 30% for non-core industries)
- Those who perceive protecting privacy as important (40%)
- Representatives at companies with higher awareness of privacy obligations (51%)
- Those who perceived complying with Canada's privacy laws as easy or difficult (49%)
- Those who expressed concern over a data breach (43%).

## COMPLIANCE

This section explores perceptions related to the difficulty of complying with Canada's privacy laws, including barriers to compliance.

### Privacy Compliance Seen as Neither Easy nor Difficult

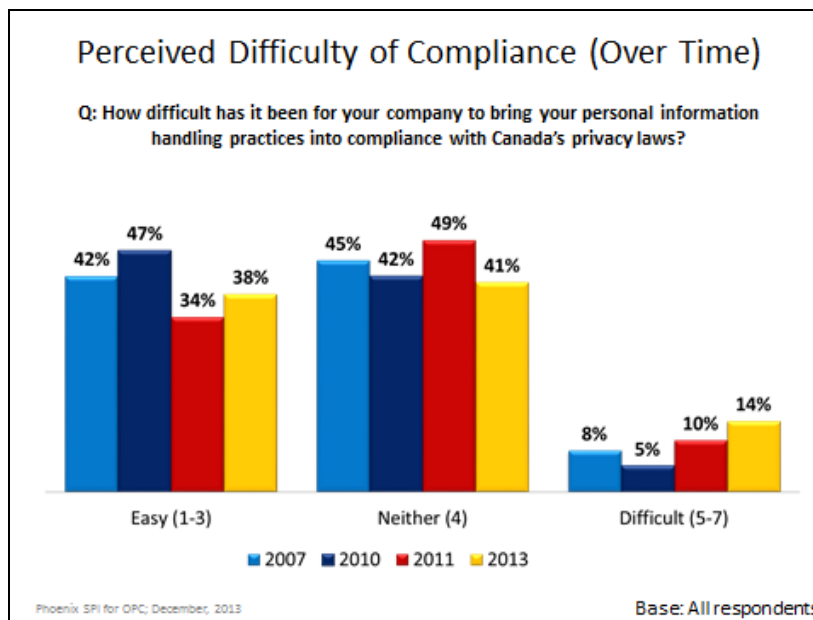
Business executives were asked how difficult it has been for their company to bring their personal information handling practices into compliance with Canada's privacy laws (using a 7-point scale: 1 = extremely easy, 7 = extremely difficult). The largest proportion (41%) were neutral, viewing this as neither easy nor difficult. Most of the rest (38%) rated compliance with Canada's privacy laws as easy, while 13% felt that this was difficult for their company.



### Subgroup Variations

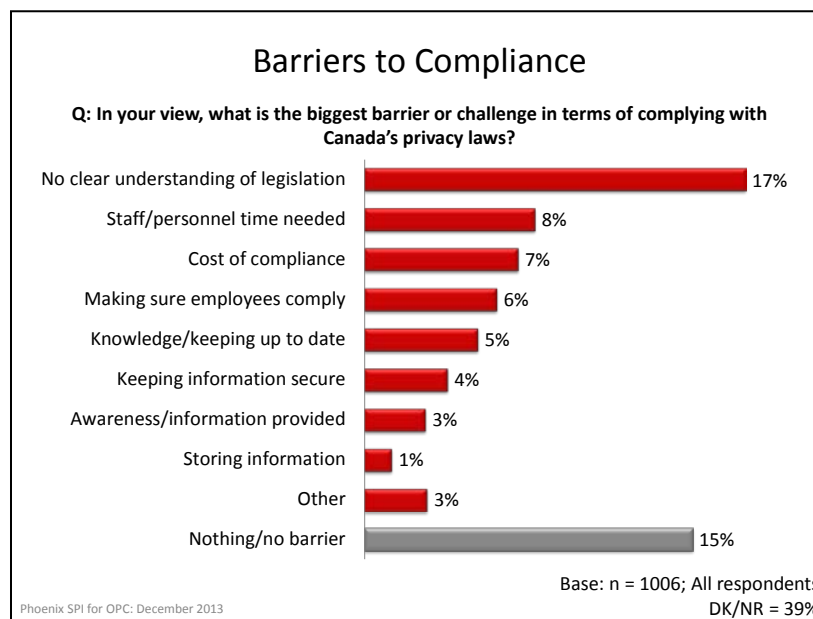
The likelihood of reporting that it has been very easy (1-2) to bring their personal information handling practices into compliance with Canada's privacy laws was higher amongst companies in core industries (35%) and those who reported being relatively aware of their privacy obligation (37%). It was lowest amongst those who perceived protecting privacy to be relatively unimportant (20% vs. 32% to 37% of companies that are neutral or privacy or see it as important).

Over time, the perceived difficulty of bringing personal information handling practices into compliance with Canada's privacy laws has increased modestly, while the perception that it is very easy has decreased. In total, 38% of business representatives currently think it is easy to comply with privacy laws—down from a high of 47% in 2010, but up slightly from 34% in 2011.



### Lack of Understanding of Legislation—Top Barrier to Compliance

A lack of understanding of privacy legislation was identified most often (17%) as the most significant barrier or challenge in terms of complying with Canada's privacy laws. Eight percent or less cited a number of other barriers: staff/personnel time needed (8%), cost of compliance (other than staff) (7%), making sure employees comply (6%), the need to keep their knowledge up to date (5%), and keeping the information secure (4%).



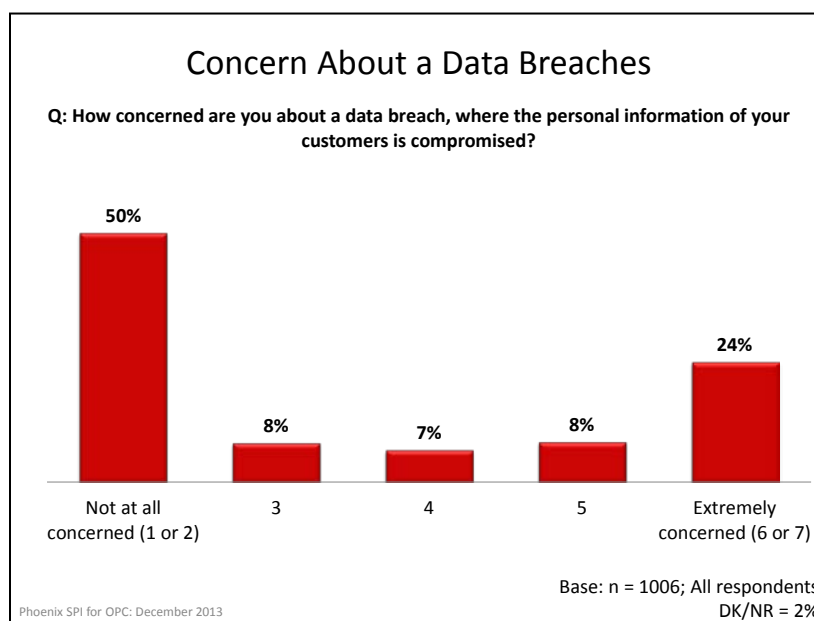
Examples included in the 'other' category, each cited by 2% or less were: keeping up to date with the law; too much paperwork/bureaucracy; barriers to accessing information; difficulties with consistently implementing policy; customer awareness; and the volume of information to protect. Fully 39% did not offer a response to this question.

## BREACHES

This section explores issues related to data breaches.

### Polarized Levels of Concern Over Data Breaches

Surveyed executives were asked to rate their level of concern about a data breach, where the personal information of their customers is compromised. They were asked to use a 7-point scale (1 = not at all concerned; 7 = extremely concerned). Exactly half (50%) said they were not at all concerned about a data breach, while 24% said they were extremely concerned. In total, exactly one-third offered scores above the mid-point of the scale, suggesting moderate concern about a data breach.



Before being asked this question, executives were provided with the following information:

*Sometimes, sensitive personal information that is held by a company about their customers is compromised. This can be due to a range of things, such as criminal activity, theft, hacking, or employee error, such as misplacing a laptop or other device.*

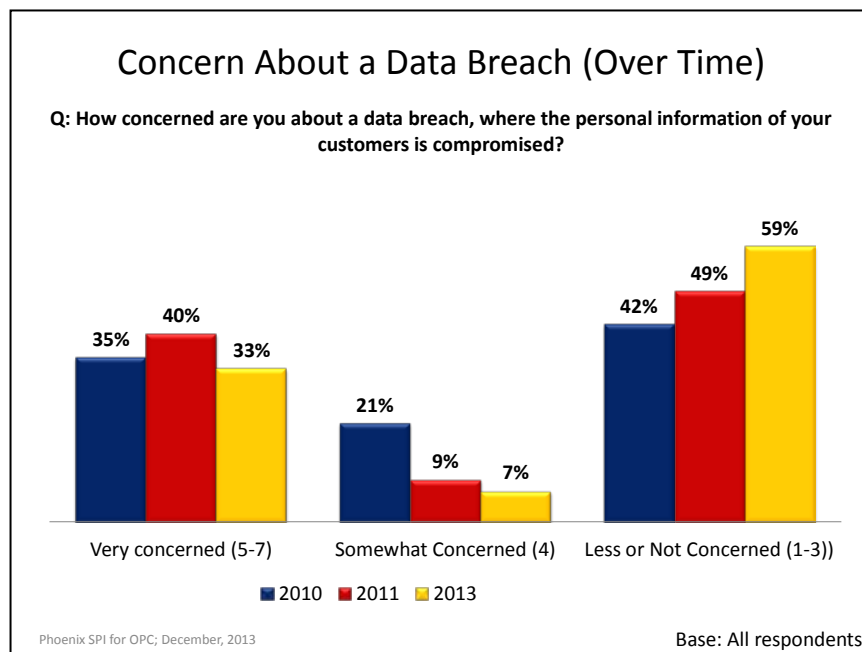
### Subgroup Variations

The likelihood of being very concerned (6-7) about a data breach was highest amongst:

- Companies located in Quebec (35%)
- Those who perceived protecting privacy as being relatively important (28%)
- Those who reported being relatively aware of their privacy obligation (30%).

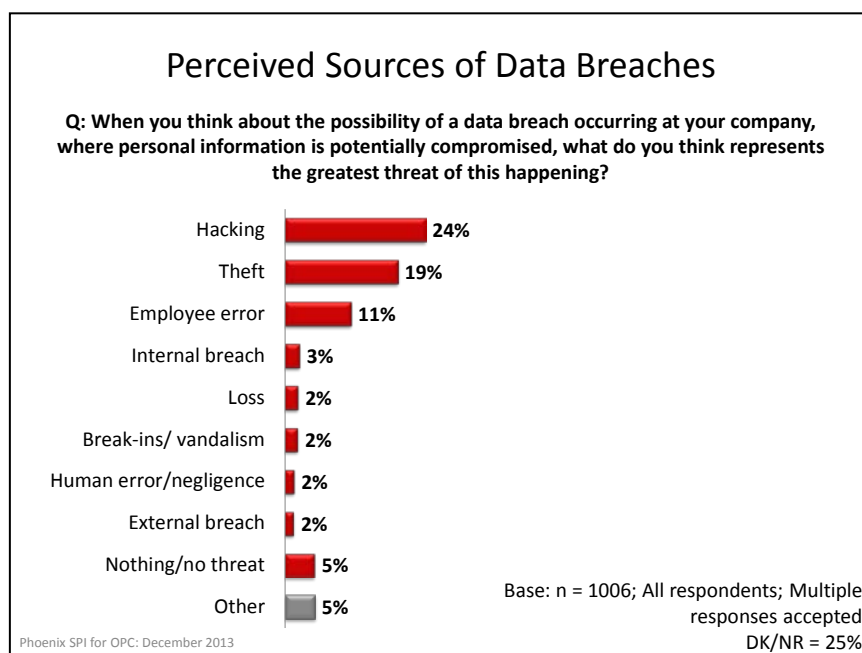
Over time, Canadian businesses have become somewhat less concerned about a data breach. Compared with 2011, the 2013 survey indicates a decrease in the proportion of businesses that are very concerned over such a breach (33% vs. 40%), as well as those

who are moderately concerned (7% vs. 9%). As a result, those with little or no concerns have increased to 59% from 49% in 2011 and 42% in 2010.



### Top Threats Leading to Breach: Hacking, Theft and Employee Error

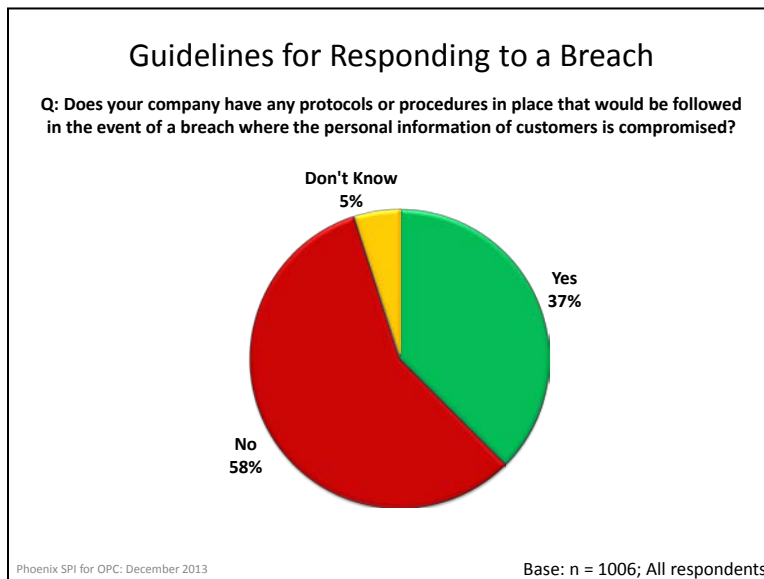
Surveyed executives were asked to think about the possibility of a data breach occurring at their company, where personal information is potentially compromised, and to identify what they think represents the greatest threat of this happening. Heading the list were hacking (24%) and theft (19%). In addition, 11% identified employee error. A number of other potential threats were identified by small numbers (3% or less).



Five percent of surveyed executives indicated that they could think of no threats, while 25% did not provide a response.

### More Than Half Do Not Have Guidelines for Responding to Breach

Fifty eight percent of surveyed companies do not have guidelines in place in the event of a breach where the personal information of their customers is compromised and 5% were unsure. Conversely, 37% do have guidelines in place.



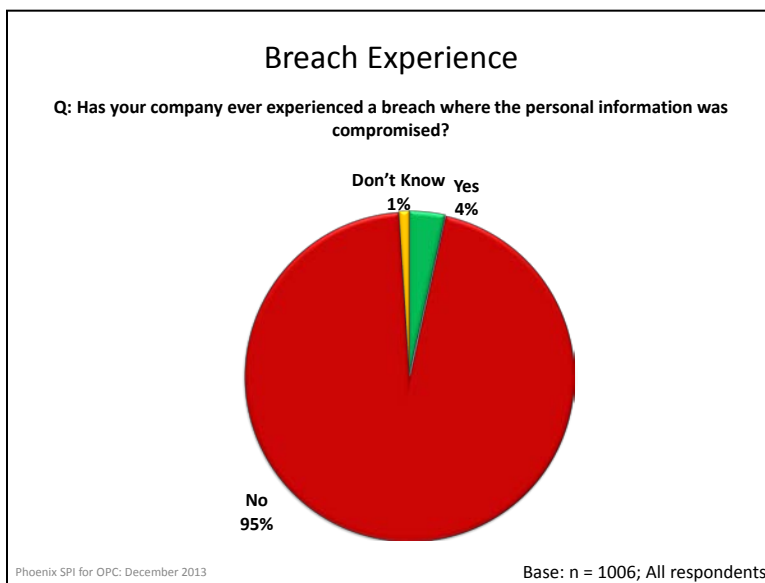
### Subgroup Variations

The likelihood of having protocols or procedures in place that would be followed in the event of a breach was highest amongst:

- Companies in the GTA (53%) and Alberta (48%)
- Companies with at least 100 employees (53%)
- Companies in core industries (45%)
- Those who perceived protecting privacy as being relatively important (43%)
- Those who reported being aware of their privacy obligations (47%)
- Those who reported being relatively concerned over a data breach (44%).

## Relatively Few Say They Have Ever Experienced a Breach

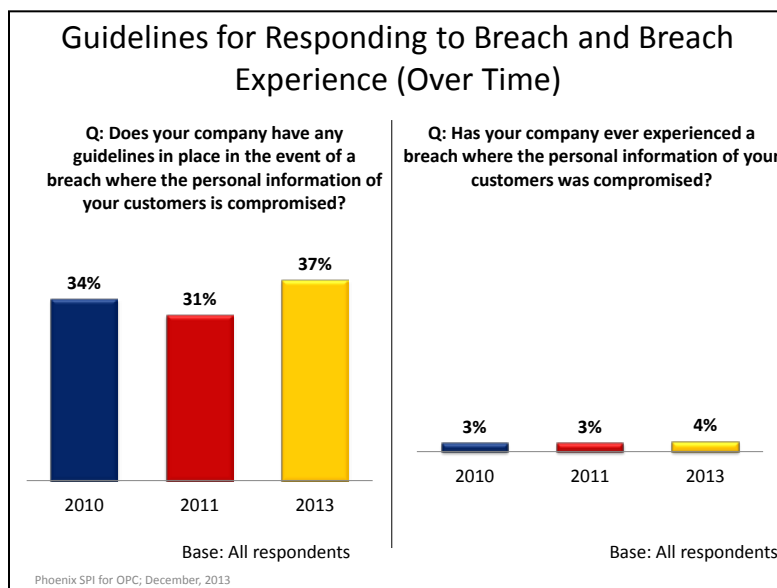
The vast majority (95%) of businesses say they have never experienced a breach where the personal information of their customers was compromised. Conversely, only 4% have (1% were unsure).



## Subgroup Variations

Larger companies were more likely than smaller ones to report having experienced a data breach where the personal information was compromised (11% of companies with at least 100 employees vs. 1% and 5% of small- and medium-sized companies).<sup>5</sup>

The proportion of companies who have guidelines in place to respond to a breach has increased modestly since 2011 (31%) and 2010 (34%)<sup>6</sup>. The number of companies (4%) who have actually experienced a data breach has remained virtually unchanged since 2011 and 2010 (3% each).



<sup>5</sup> Caution should be exercised interpreting these findings due to some small sample sizes.

<sup>6</sup> In 2013, the question wording was changed to ask about "any protocols or procedures in place" versus "any guidelines in place" in 2011 and 2010.



In total, fifty-two respondents said their company had experienced a breach. The most common steps taken by these companies to address the situation was notifying individuals who were affected, followed by resolving the issue with the individual responsible for the breach and enhancing their security system. Others said they provided training to their staff, reviewed their privacy policy, notified law enforcement, notified the relevant government agencies, took legal action, obtained information from the government, or notified relevant departments within the company. Eight percent of companies pursued other means of addressing the breach.

## CORPORATE INNOVATION

This section addresses companies' use of third parties for processing, storage, and other services with relation to customers' personal information.

### Policies in Place to Assess Privacy Risks

When asked whether their companies have policies in place to assess privacy risks related to their business, approximately two-thirds (67%) said that they do not, while 5% were uncertain.



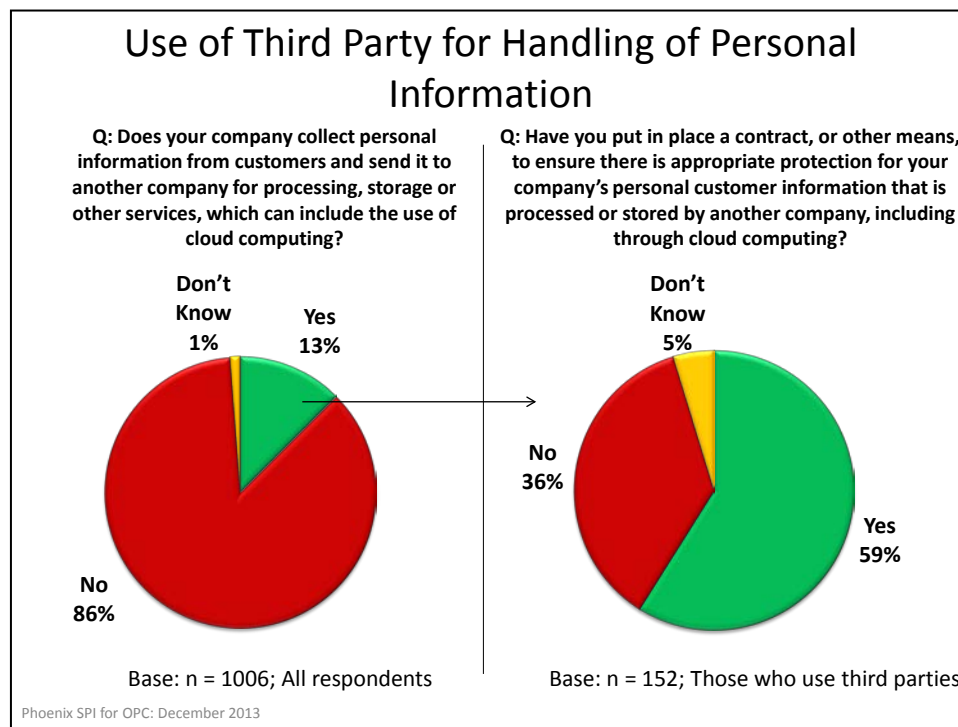
### Subgroup Variations

The likelihood of a company having policies or procedures in place to assess privacy risks was highest amongst:

- Companies that sell to both consumers and businesses (33%)
- Larger companies (46%)
- Companies in core industries (32%)
- Those who perceived protecting privacy as being relatively important (32%)
- Those who reported being relatively aware of their privacy obligation (35%).

## Use of Third Parties to Manage Personal Information

Only 13% of surveyed businesses send customer's personal data to a third party for processing, storage or other services. Of this 13%, 59% claimed to be aware that when a company transfers personal information to a third party for processing, storage or other services, which can include the use of cloud computing, that a company remains accountable for that information. Conversely, 36% were not aware of this accountability.

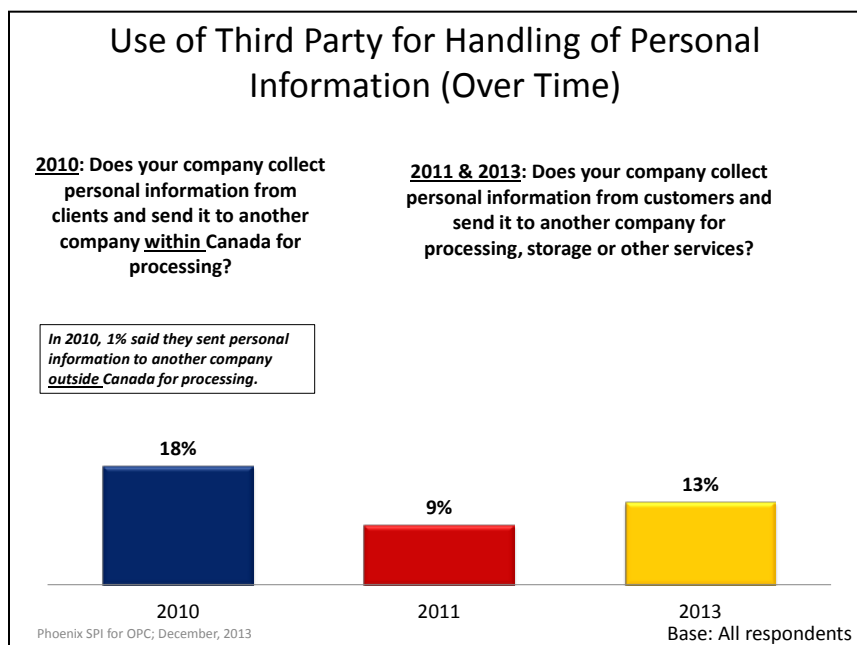


### Subgroup Variations

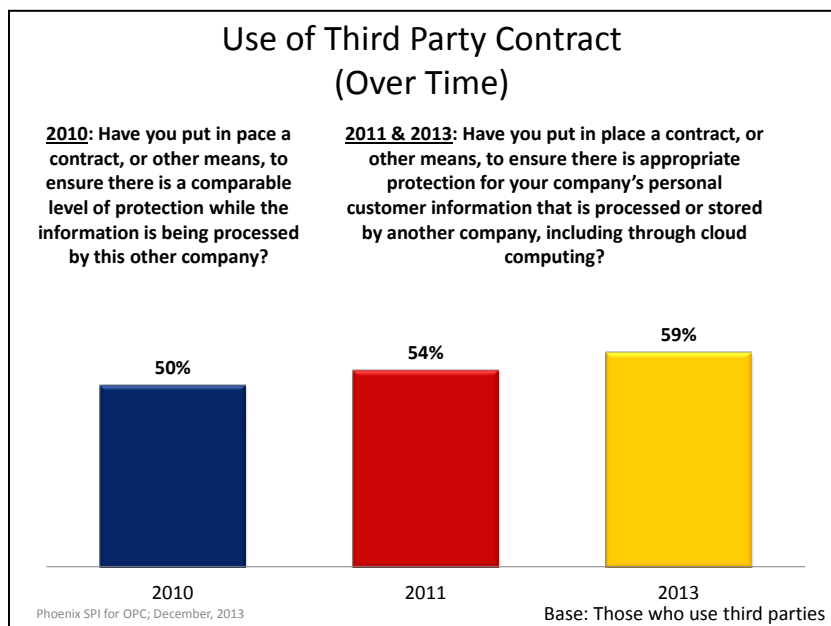
The likelihood of a company sending their customers' personal information to another company for processing, storage or other services was highest amongst<sup>7</sup>: companies with at least 100 employees (24%) and companies in core industries (16%).

<sup>7</sup> Caution should be exercised interpreting these findings due to some small sample sizes.

In 2013, a larger proportion (13%) of companies used third parties than in 2011 (9%). However, this is still down from 2010 when 18% of respondents said a third party is responsible for handling personal information.<sup>8</sup>



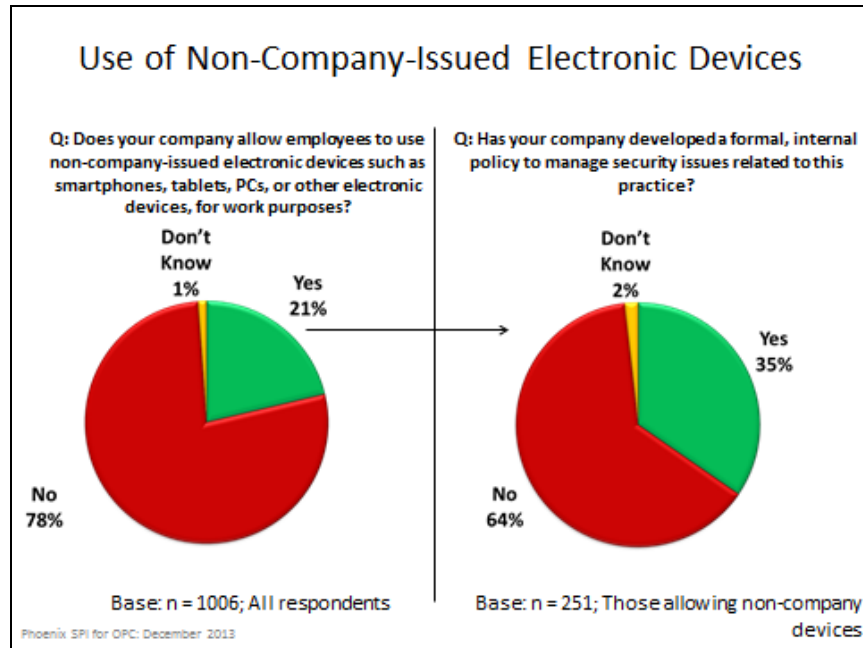
The number of companies with contracts in place to ensure customers' information is protected by the third party has steadily increased since 2010.



<sup>8</sup> In 2010, the question asked only about using third party for information processing, whereas in 2011 it included processing, storage, or other services.

## Use of Non-Company-Issued Electronic Devices

Business representatives were asked about their company's policy on allowing employees to use their personal electronic devices, such as smartphones, tablets or laptops, for work purposes. Approximately one in five (21%) companies allow this. Of the 21% (or 251 respondents), two in three (64%) have not developed formal, internal policies to manage security issues related to employees using their own devices for work. Two percent of respondents were unsure of their company's policy.



### Subgroup Variations<sup>9</sup>

The likelihood of allowing employees to use non-company-issued electronic devices for work purposes was highest amongst:

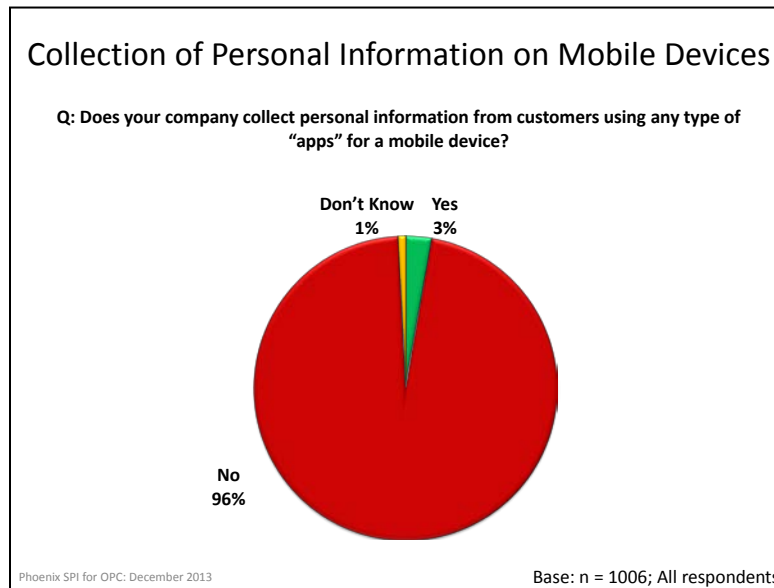
- Companies in the GTA (32%) and BC (31%)
- Companies that sell only to businesses (27%)
- Companies with 20+ employees.

Larger companies were more likely to have developed a formal, internal policy to manage security issues related to this practice (62% with at least 100 employees vs. 42% or fewer of smaller companies).

<sup>9</sup> Caution should be exercised interpreting these findings due to some small sample sizes.

## Collection of Customer information on Mobile Devices

The vast majority of companies (96%) do not collect customers' personal information using apps on mobile devices, with only 3% of business representatives stating that their company does collect such data.



Among the thirty-four firms that collect information on mobile devices, the majority collect contact information, such as names, phone numbers, and addresses. Smaller numbers collect location information, record customers' opinions, evaluations, and comments, as well as collect financial information, data on customers' purchasing habits, or some other form of personal information.

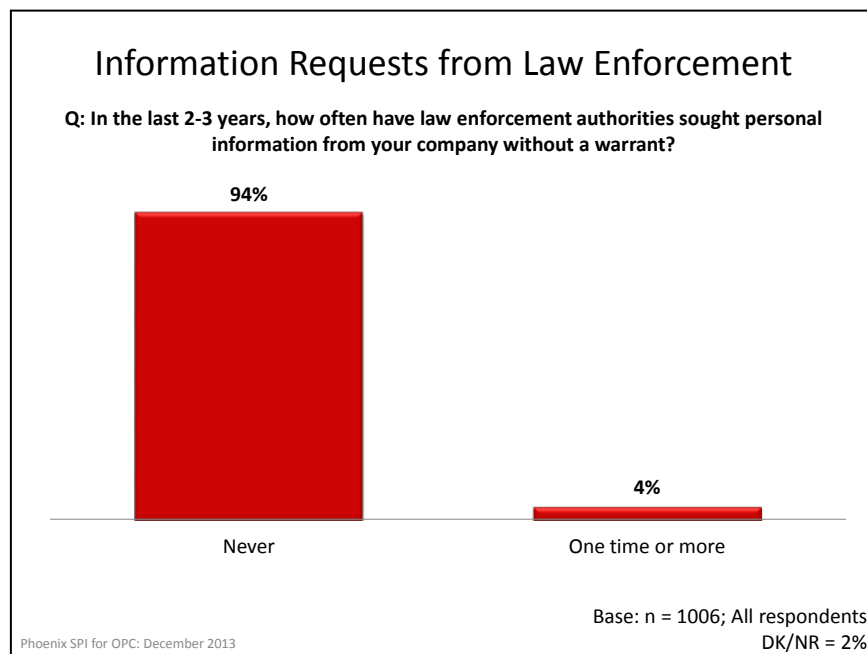
The two most common ways that these companies inform customers that their data will be collected are through the company's general privacy policy and a privacy policy that is specific to the 'app'. Approximately two in five representatives of companies that record customer data do not know how their company informs customers.

## DISCLOSURES TO LAW ENFORCEMENT

This section addresses issues relating to the extent of companies' cooperation with law enforcement in accordance with privacy laws.

### Warrant-less Requests for Personal Information

Very few companies (4%) say they have received requests from law enforcement representatives without a warrant for personal information in the last 2–3 years.



Among the sixty-two companies<sup>10</sup> that received such requests, approximately half (48%) provided the information each time it was requested. Relatively few (13%) did so some of the time. Conversely, exactly four in ten said they never provided the requested information.

<sup>10</sup> When absolute numbers are reported, these numbers are always unweighted—in other words, they represent the actual number of respondents who were asked a survey question. The weighted number of respondents asked this question is 42.

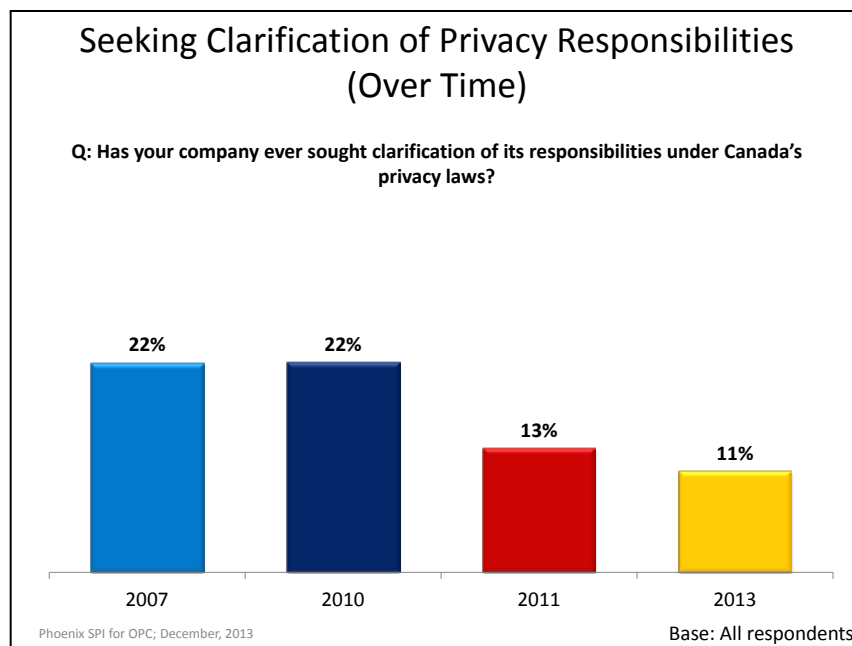
## SEEKING CLARIFICATION ABOUT RESPONSIBILITIES UNDER THE LAW

This section presents participant feedback on the sources and channels their companies use to gather information relating to privacy issues.

### Internet—Top Potential Source of Information on Privacy Laws

A majority of business representatives surveyed (86%) indicated that their company has never sought clarification of its responsibilities under privacy laws in Canada. Approximately one in ten companies have sought clarification (11%), and four percent of employees surveyed were uncertain.

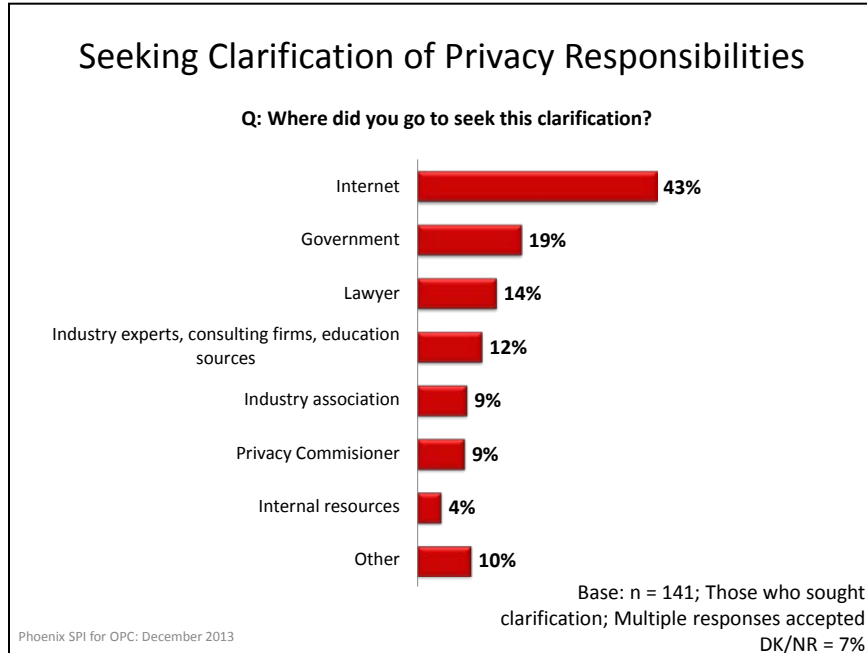
The proportion of companies (11%) that sought clarification on their responsibilities under Canada's privacy laws in 2013 is lower than in 2011 (13%), 2007 (22%), and 2010 (22%).



### Subgroup Variations

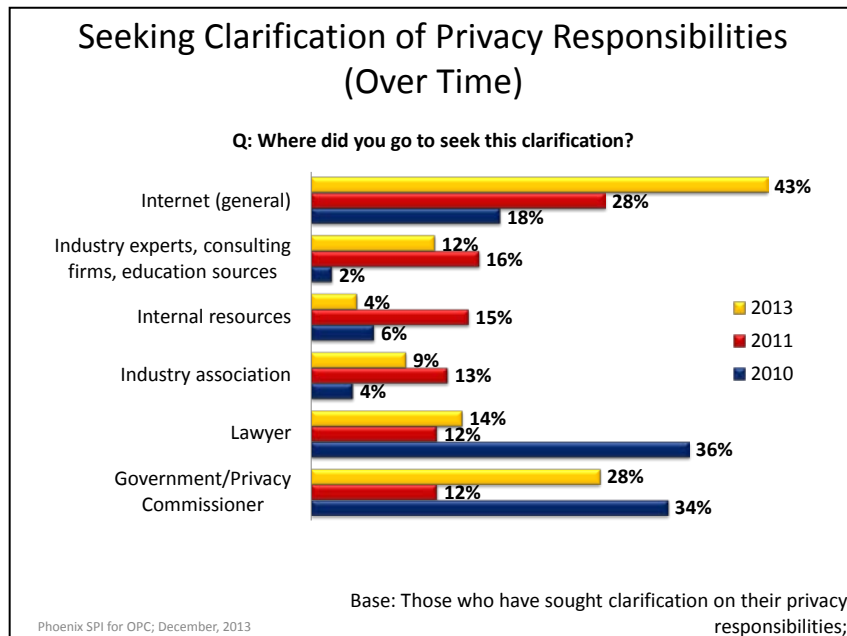
The likelihood of having sought clarification of its responsibilities under Canada's privacy laws was highest amongst larger companies (28%), those that perceived protecting privacy as being important (13%), those who reported being relatively aware of their privacy obligations (15%), and those who perceived compliance with privacy laws as being relatively difficult (21%).

In total, 141 companies have sought clarification of their privacy responsibilities. The Internet, mentioned by 43% of these firms, was the main information source. Following this, 19% have gone to government agencies (federal, provincial, or general), 14% have sought the advice of a lawyer, 12% consulted industry experts, consulting firms or education sources, 9% asked an industry association, 9% contacted the privacy commissioner, and 4% used their company's internal resources.



One in ten (10%) business representatives sought clarification from some other source, and 7% were unsure of where they went for clarification.

Where executives go for clarification on privacy laws has changed substantially since tracking began in 2010.



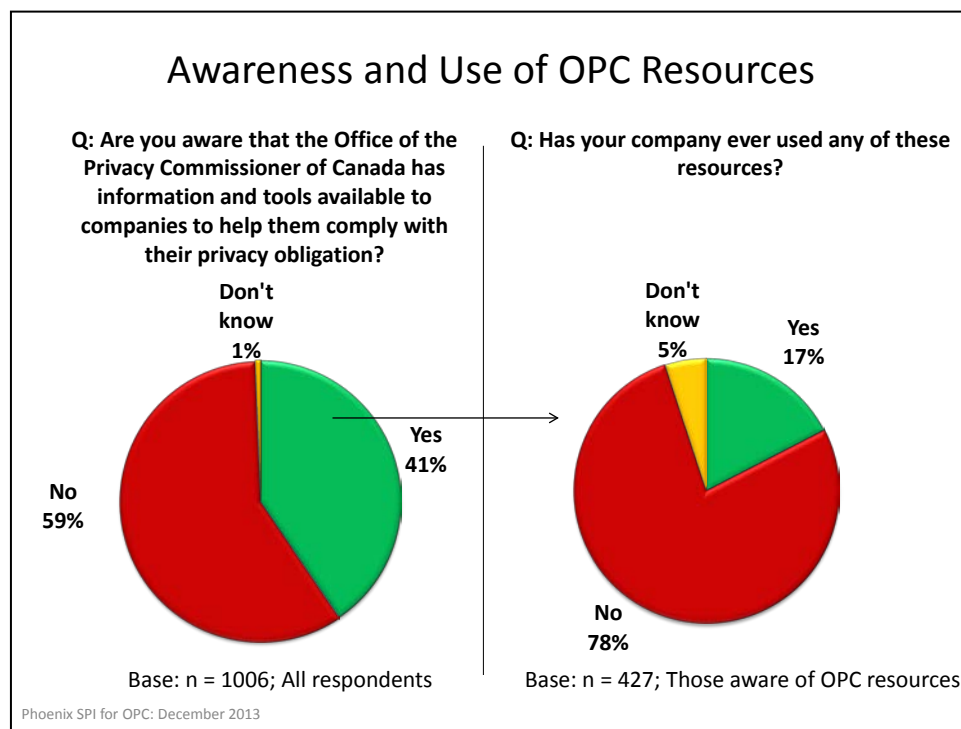
## OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

This section explores levels of awareness of resources available through the Office of the Privacy Commissioner (OPC), as well as use of such resources and assessments of them.

### Strong Minority Aware of OPC Resources, Most Have Not Used Resources

Forty-one percent of surveyed executives said they were aware that the OPC has information and tools available to companies to help them comply with their privacy obligations.

However, among executives who are aware of OPC resources, the majority (78%) have never used them. Close to one in five (17%) have used OPC resources and five percent of respondents were uncertain as to whether their company has used them.



### Subgroup Variations

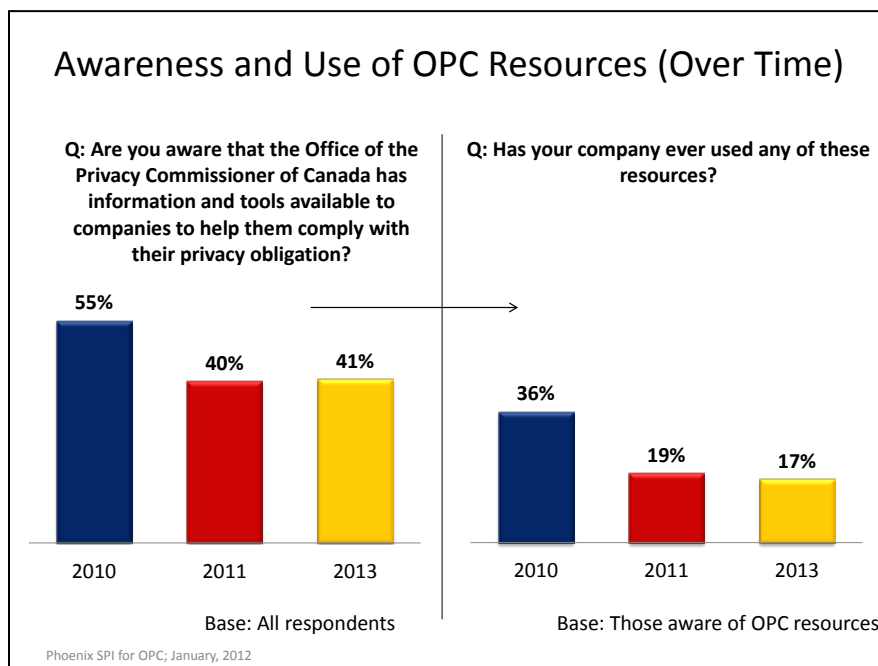
The likelihood of being aware that OPC has resources available was highest amongst<sup>11</sup>:

- Companies located in the Prairies (63%) and Alberta (56%)
- Companies that sell to both consumers and businesses (48)
- Companies with at least 100 employees (53%)
- Those who perceived protecting privacy as being important (44%)
- Those who reported being aware of their privacy obligations (48%).

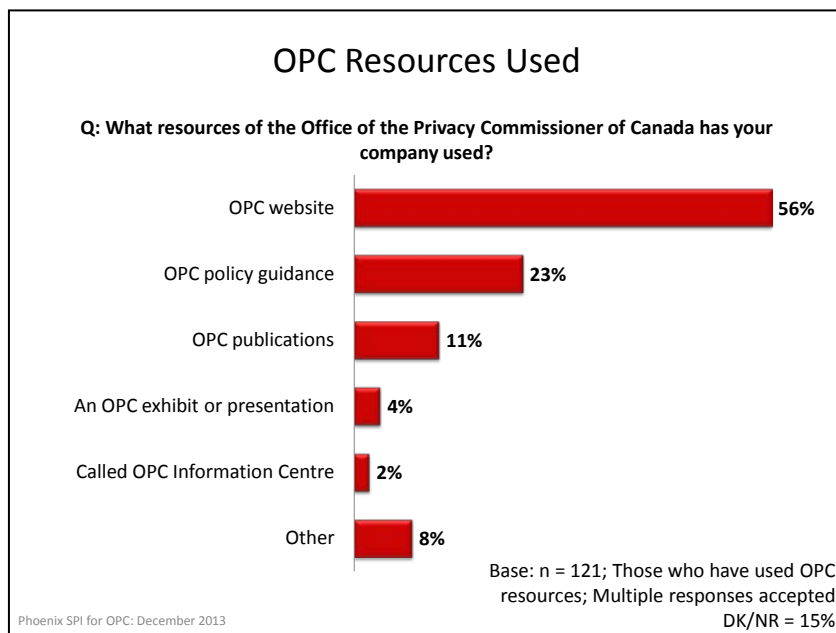
Larger companies and those who reported their company is aware of privacy obligations were more likely to have used OPC resources.

<sup>11</sup> Caution should be exercised interpreting these findings due to some small sample sizes.

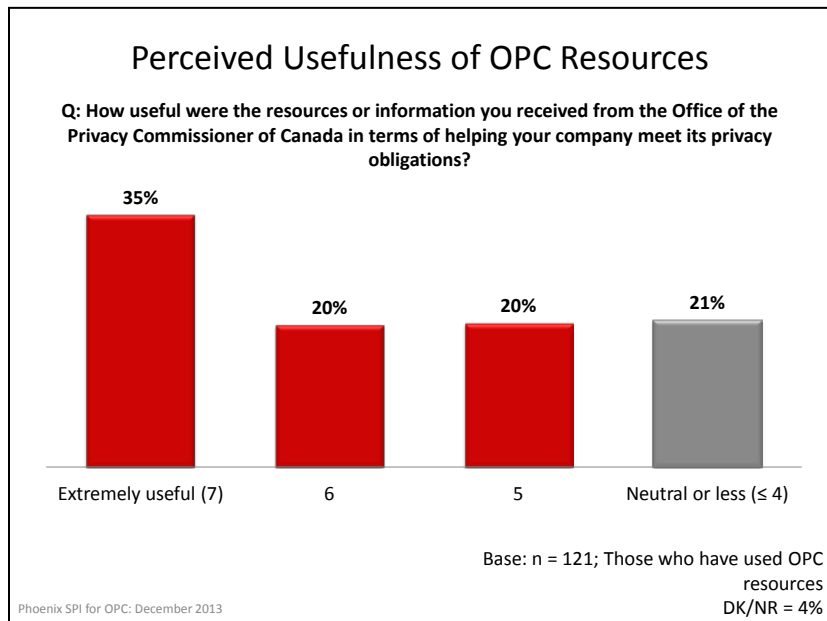
Awareness and use of OPC resources is virtually unchanged since 2011.



Among the 121 companies that have used OPC resources to comply with their privacy obligations, the OPC website (56%) was the main source of reference. The survey found that 23% used OPC policy guidance, 11% OPC publications, 4% an OPC exhibit or presentation, and only 2% called the OPC information centre. Eight percent of companies used some other source of information from the OPC. Fifteen percent of business representatives were uncertain of which OPC resource their company used.

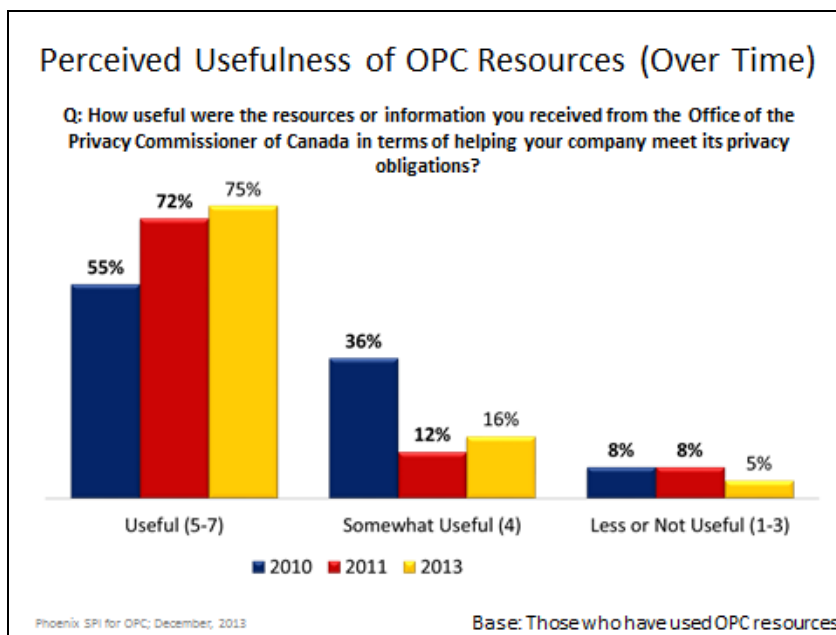


Executives were asked to rate the usefulness of privacy-related resources they received from the OPC on a seven-point scale (7 = extremely useful, 1 = not at all useful). Exactly three-quarters of executives rated their usefulness above the midpoint of the seven-point scale, with 35% stating that they were extremely useful.



The five respondents who offered low assessments of the usefulness of OPC resources (scores of 1-3) were asked why they found the resources or information not very useful. Reasons included that they already knew the information or that the information was not appropriate for their business size.

The perceived usefulness of OPC resources among business representatives has increased since tracking began in 2010.



## CORPORATE PROFILE

The following table presents the characteristics of survey respondents (using weighted data).

Region	Percent
Atlantic Canada	7%
Quebec	20%
Manitoba and Saskatchewan	7%
Alberta	14%
British Columbia	16%
Ontario (excluding the Greater Toronto Area)	21%
Greater Toronto Area	14%
Don't know / no response	1%
Total	100%

Business Size	Percent
Self-employed (1 employee)	14%
Small (2-19 employees)	74%
Medium (20-99 employees)	10%
Large (100+ employees)	2%
Total	100%

Language of interview	Percent
English	80%
French	20%
Total	100%

Revenues in 2012	Percent
Less than \$100,000	16%
\$100,000 to just under \$250,000	13%
\$250,000 to just under \$500,000	10%
\$500,000 to just under \$1,000,000	13%
\$1,000,000 to just under \$5,000,000	19%
\$5,000,000 to just under \$10,000,000	4%
\$10,000,000 to just under \$20,000,000	2%
More than \$20 million	2%
Don't know / no response	22%
Total	100% <sup>12</sup>

<sup>12</sup> Total does not sum to 100% due to rounding error.



## APPENDIX

## TELEPHONE QUESTIONNAIRE

*Note: Some questions in the questionnaires are indicated as having been deleted. This reflects changes made to the questionnaire following the pre-test in order to reduce the length of the survey.*

Hello, my name is \_\_\_\_\_. I'm calling on behalf of Phoenix, a public opinion research company. We're conducting a survey for the Privacy Commissioner of Canada to better understand the needs and practices of businesses across the country 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.

- ☐ IF PERSON IS AVAILABLE, CONTINUE. REPEAT INTRODUCTION IF NEEDED.
- ☐ IF NOT AVAILABLE, SCHEDULE CALL-BACK.

The survey takes about 15 minutes and is voluntary and completely confidential. Your answers will remain anonymous. May I continue?

- [ ] Yes, now (CONTINUE)
- [ ] No, call later. Specify date/time:      Date:      Time:
- [ ] Refused (THANK & DISCONTINUE)

### INTERVIEWER NOTES:

IF RESPONDENT ASKS ABOUT THE LENGTH OF THE SURVEY, INFORM HIM/HER IT SHOULD TAKE APPROXIMATELY 15 MINUTES.

IF RESPONDENT QUESTIONS THE VALIDITY OF THE SURVEY, ASK HIM/HER TO CALL HEATHER ORMEROD OF THE OFFICE OF THE PRIVACY COMMISSIONER AT 613-947-8416 (OR HAVE HEATHER CALL THE RESPONDENT). OR THE RESPONDENT CAN CALL THE NATIONAL SURVEY REGISTRATION SYSTEM (SEE BELOW).

IF RESPONDENT ASKS, THE SURVEY IS REGISTERED WITH THE NATIONAL SURVEY REGISTRATION SYSTEM:

The registration system has been created by the survey research industry to allow the public to verify that a survey is legitimate, get information about the survey industry or register a complaint. The registration system's toll-free phone number is 1-888-602-6742 ext. 8728.

SOME QUESTIONS ARE TRACKING QUESTIONS THAT WERE USED IN EARLIER SURVEYS. TRACKING QUESTIONS ARE IDENTIFIED AS FOLLOWS: T2011 = TRACKING (T) FROM THE 2011 BUSINESS SURVEY.

HEADINGS IN BLUE SHOULD NOT BE READ TO RESPONDENTS

FOR ALL QUESTIONS, INCLUDE 'DON'T KNOW/NO RESPONSE' OPTION

1. Which of the following best describes your company? (READ LIST, ACCEPT ONE RESPONSE) T2011

- |  |   |
|--|---|
| It sells directly to consumers   | 1 |
| It sells directly to other businesses/organizations                    | 2 |
| It sells directly both to consumers and other businesses/organizations | 3 |
| Other, please specify: _____   |   |



(DO NOT READ: NOT FOR PROFIT, THANK AND TERMINATE;  
DK/NR, THANK AND TERMINATE)

2. Approximately how many employees work for your company in Canada? Please include part-time employees as full-time equivalents. (DO NOT READ LIST) T2011

One (i.e. self employed)	1
2-4	2
5-9	3
10-19	4
20-49	5
50-99	6
100-149	7
150-199	8
200-249	9
250-299	10
300-499	11
500-999	12
1,000-4,999	13
More than 5,000	14

#### SECTION 1: PRIVACY PRACTICES

I'd like to begin by asking you about the types of personal information held by your company about your customers. T2011 MODIFIED

3. Which of the following types of personal information does your company collect about your customers? (READ LIST. ACCEPT ALL THAT APPLY) T2011

Contact information, such as names, phone numbers, and addresses	1
Opinions, evaluations, and comments	2
Purchasing habits	3
Financial	4
Medical information	5
Location information, such as postal codes	6
Other information. If so, please specify: _____	
None of the above (DO NOT READ)	7

4. What does your business do with the personal information that it collects about your customers? Do you use it for...? (READ LIST. ACCEPT ALL THAT APPLY)

- a. Marketing
- b. Providing service
- c. Building customer profiles to personalize service
- d. Or for some other purpose. If so, please specify: \_\_\_\_\_

5. Deleted

6. Deleted



7. In which of the following ways does your company store personal information on your customers? Is the information...? (READ LIST. ACCEPT ALL THAT APPLY) T2011

Stored on-site on paper	1
Stored on-site on servers	2
Stored on desktop computers	3
Stored on portable devices, such as laptops, USB sticks, or tablets	4
Stored electronically through cloud computing*	5
Stored through a third party, not including cloud computing**	6
Stored by video and audio recordings	7
Stored in some other way: If so, please specify _____	8

\*INTERVIEWER NOTE: IF RESPONDENT IS NOT CLEAR WHAT CLOUD COMPUTING IS, SAY THAT CLOUD COMPUTING REFERS TO THE DELIVERY OF COMPUTING RESOURCES OVER THE INTERNET. INSTEAD OF KEEPING DATA ON YOUR OWN HARD DRIVE OR UPDATING APPLICATIONS FOR YOUR NEEDS, YOU USE A THIRD PARTY'S SERVICE OVER THE INTERNET, AT ANOTHER LOCATION, TO STORE YOUR INFORMATION OR USE ITS APPLICATIONS.

\*\*INTERVIEWER NOTE: FOR THIS QUESTION, CLOUD COMPUTING SHOULD BE RECORDED SEPARATELY FROM STORAGE BY A THIRD PARTY.

IF INFORMATION 'STORED ON PORTABLE DEVICES', ASK:

8. Does your company use encryption to protect the personal information you store on portable devices, such as laptops, USB sticks, or tablets? T2011

Yes	1
No	2

ASK EVERYONE:

9. What steps do you take to protect the personal information on your customers? (READ LIST. ACCEPT ALL THAT APPLY) T2011

Physical measures, such as locked filing cabinets, restricting access, or security alarms.	1
Technological tools, such as passwords, encryption, or firewalls.	2
Organizational controls, such as policies and procedures.	3
Some other measure. If so, please specify: _____	4
No measures taken	5

IF 'TECHNOLOGICAL TOOLS' USED, ASK:

10. What technological tools do you use? (READ LIST. ACCEPT ALL THAT APPLY) T2011 MODIFIED

Passwords	1
Encryption	2
Firewalls	3
Other. Please specify: _____	

IF 'PASSWORDS' USED, ASK NEXT TWO QUESTIONS:

11. How often do you require employees to change their passwords? (DO NOT READ LIST. ACCEPT ONE RESPONSE) T2011

Monthly	1
Quarterly	2
Every six months	3
Once a year	4
Less than this	5
VOLUNTEERED: Do not require employees to change passwords	6

12. Do you have any controls in place to ensure that employees use hard-to-guess passwords? T2011

Yes	1
No	2

ASK EVERYONE:

13. Have you designated someone in your company to be responsible for privacy issues and personal information that your company holds? T2011

Yes	1
No	2

14. Has your business developed and documented internal policies for staff that address your privacy obligations under the law?

Yes	1
No	2

15. Does your organization regularly provide staff with privacy training and education?

Yes	1
No	2

16. Does your company have procedures in place for responding to customer requests for access to their personal information? T2011

Yes	1
No	2

17. Does your company have procedures in place for dealing with complaints from customers who feel that their information has been handled improperly? T2011

Yes	1
No	2



18. Does your company have a privacy policy that explains to customers how you will collect and use their personal information? T2011 MODIFIED

Yes	1
No	2

## SECTION 2: PRIVACY AS CORPORATE OBJECTIVE

19. What importance does your company attribute to protecting your customers' personal information? Please use a scale from 1 to 7, where 1 means that this is not an important corporate objective at all, and 7 means it is an extremely important objective. T2011 MODIFIED

20. Deleted

21. How confident are you that your company knows how to fully protect the personal information you collect? Would you say very confident, moderately, not very or not confident at all?

## SECTION 3: AWARENESS AND IMPACT OF PRIVACY LAWS

The federal government's privacy law, the *Personal Information and Protection and Electronic Documents Act* or PIPEDA (PRONOUNCED PIP-EE-DAH) sets out rules that govern how businesses engaged in commercial activities should protect personal information. In Alberta, BC and Quebec, the private sector is governed by provincial laws, which are considered to be similar to the federal law. T2011

22. How would you rate your company's awareness of its responsibilities under Canada's privacy laws? Please use a scale from 1 to 7, where 1 is not at all aware, and 7 is extremely aware. T2011

23. And thinking specifically about PIPEDA (PRONOUNCED PIP-EE-DAH), the federal government's privacy law, how would you rate your company's awareness of this legislation? Please use a scale from 1 to 7, where 1 is not at all aware, and 7 is extremely aware. T2011

## SECTION 4: COMPLIANCE

24. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Please use a scale from 1 to 7, where 1 is extremely easy, 7 extremely difficult and 4 is neither easy nor difficult. T2011

25. In your view, what is the most significant barrier or challenge in terms of complying with Canada's privacy laws? (DO NOT READ LIST. ACCEPT MULTIPLE RESPONSES) T2011 MODIFIED

Don't have a clear understanding of the legislation	1
Staff/personnel time needed	2
Cost of compliance (non-staff costs)	3
Other: Specify _____	

26. Deleted

## SECTION 5: BREACHES

Sometimes, sensitive personal information that is held by a company about their customers is compromised. This can be due to a range of things, such as criminal activity, theft, hacking, or employee error such as misplacing a laptop or other device. T2011 MODIFIED

27. How concerned are you about a data breach, where the personal information of your customers is compromised? Please use a scale of 1 to 7, where 1 is not at all concerned, and 7 is extremely concerned. T2011

28. When you think about the possibility of a data breach occurring at your company, where personal information is potentially compromised, what do you think represents the greatest threat of this happening? (DO NOT READ LIST. ACCEPT ONE RESPONSE)

Hacking	1
Theft	2
Loss	3
Use of mobile devices by employees	4
Employee error	5
Other: Specify _____	

29. Does your company have any protocols or procedures in place that would be followed in the event of a breach where the personal information of customers is compromised? T2011 MODIFIED

Yes	1
No	2

30. Has your company ever experienced a breach where personal information was compromised? T2011 MODIFIED

Yes	1	
No	2	SKIP NEXT QUESTION



ASK THOSE WHO HAVE EXPERIENCED A BREACH:

31. What did your company do to address this situation? (DO NOT READ LIST. ACCEPT MULTIPLE RESPONSES) T2011

Notified individuals who are affected	1
Notified government agencies who oversee Canada`s privacy laws	2
Notified law enforcement	3
Followed proper procedure (general)	4
Notified company`s head office, HR, or privacy department	5
Obtained legal counsel/took legal action	6
Resolved issue with individuals responsible for the breach (e.g. termination/reprimand of employee)	7
Obtained information from government (websites, 1-800 number)	8
Issued training or re-training for staff	9
Reviewed privacy policy or practices	10
Implemented security system or enhanced security	11
Other (specify): _____	12

32. Deleted

**SECTION 6: CORPORATE INNOVATION**

33. Does your company have any policies or procedures in place to assess privacy risks related to your business? This includes assessing privacy risks associated with the development or use of new products, services, or technologies. T2011

Yes	1
No	2

34. Does your company collect personal information from customers and send it to another company for processing, storage or other services, which can include the use of cloud computing? T2011 [NOTE INCONSISTENCIES WITH Q7 AND PROBE FOR THE CORRECT ANSWER TO BOTH QUESTIONS].

Yes	1
No	2

ASK ONLY THOSE WHO USE THIRD PARTY (Q34):

35. Have you put in place a contract, or other means, to ensure there is appropriate protection for your company's personal customer information that is processed or stored by another company, including through cloud computing\*? T2011

Yes	1
No	2

\*ONLY INCLUDE "INCLUDING THROUGH CLOUD COMPUTING" FOR THOSE WHO CURRENTLY USE CLOUD COMPUTING.



36. Does your company allow employees to use non-company-issued electronic devices, such as smartphones, tablets, PCs, or other electronic devices, for work purposes?

Yes	1	
No	2	GO TO Q38

IF 'YES', ASK:

37. Has your company developed a formal, internal policy to manage security issues related to this practice?

Yes	1
No	2

38. Does your company collect personal information from customers using any type of “apps” for a mobile device?

Yes	1
No	2

IF 'YES', ASK NEXT TWO QUESTIONS:

39. Which of the following types of information does your company collect through your “apps”? (READ LIST. ACCEPT ALL THAT APPLY)

Contact information, such as names, phone numbers, and addresses	1
Opinions, evaluations, and comments	2
Purchasing habits	3
Financial information, including credit card numbers	4
Location information	5
Other information. If so, please specify: _____	
None of the above (DO NOT READ)	6

40. How does your company communicate to users the purposes for which information collected via the app will be used?

In your company's general privacy policy	1
In a privacy policy specific to the app	2
In the app distribution “store”	3
Using in-app notifications	4
Other. Please specify: _____	5

## **SECTION 7: COOPERATION WITH LAW ENFORCEMENT AND GOVERNMENT**

Under Canada’s privacy laws, if law enforcement agencies have a warrant from the court, they can require a company to disclose the personal information it holds about its customers. When they do not have a warrant, a company can provide or refuse to provide the information.



41. In the last 2-3 years, how often have law enforcement authorities sought personal information from your company without a warrant? (READ LIST. ACCEPT ONE RESPONSE)

- Never
- 1-5 times
- 6-10 times
- More than 10 times

IF INFO REQUESTED (PREVIOUS QUESTION), ASK:

42. Did your company comply and provide the requested information...? (READ LIST. ACCEPT ONE RESPONSE)

- Each time it was requested
- Some of the time
- None of the times

## SECTION 8: COMMUNICATIONS

43. Deleted

44. Deleted

45. Has your company ever sought clarification of its responsibilities under Canada's privacy laws? T2011

- |     |   |                    |
|-----|---|--------------------|
| Yes | 1 |                    |
| No  | 2 | SKIP NEXT QUESTION |

IF YES, ASK:

46. Where did you go to seek this clarification? (DO NOT READ LIST. ACCEPT MULTIPLE RESPONSES) T2011

- |  |    |
|--|----|
| Internet (general)                                       | 1  |
| Government   | 2* |
| [PROBE WHETHER FEDERAL (2A) OR PROVINCIAL (2B)]          |    |
| Privacy Commissioner                                     | 3* |
| [PROBE WHETHER FEDERAL (3A) OR PROVINCIAL (3B)]          |    |
| Lawyer   | 4  |
| Company/head office expert/internal resource for company | 5  |
| Industry experts, consulting firms, or education sources | 6  |
| Industry association                                     | 7  |
| Other. Specify: _____                                    |    |

# SECTION 9: OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

47. Are you aware that the Office of the Privacy Commissioner of Canada has information and tools available to companies to help them comply with their privacy obligations?  
T2011 MODIFIED

Yes	1	
No	2	GO TO NEXT SECTION

IF YES, ASK:

48. Has your company ever used any of these resources? T2011

Yes	1	
No	2	GO TO NEXT SECTION

IF YES, ASK:

49. What resources of the Office of the Privacy Commissioner of Canada has your company used? (DO NOT READ LIST. ACCEPT MULTIPLE RESPONSES) T2011 MODIFIED

OPC website	1
OPC publications	2
OPC policy guidance/advice	3
An OPC exhibit or presentation	4
Called OPC Information Centre (for enquiries)	5
Other (specify): _____	

50. How useful were the resources or information you received from the Office of the Privacy Commissioner of Canada in terms of helping your company meet its privacy obligations? Please use a scale of 1 to 7, where 1 is not at all useful, and 7 is extremely useful. T2011

IF SCORES OF 1-3, ASK:

51. Why were the resources or information not very useful? (DO NOT READ LIST. ACCEPT MULTIPLE RESPONSES) T2011

Not enough detail	1
Too difficult to understand	2
Nothing new/already knew it	3
Not in preferred format	4
Not appropriate for business size	5
Not appropriate for business sector	6
Other (specify): _____	



## SECTION 10: CORPORATE PROFILE

These last questions are for statistical purposes only, and all answers are confidential.

52. In what industry or sector do you operate? If your company is active in more than one sector, please identify the main sector. (DO NOT READ LIST. ACCEPT ONE RESPONSE) T2011

Accommodation and Food Services	1
Administrative & Support, Waste Management and Remediation Services	2
Agriculture, Forestry, Fishing and Hunting	3
Arts, Entertainment and Recreation	4
Construction	5
Educational Services	6
Finance and Insurance	7
Health Care and Social Assistance	8
Information and Cultural Industries	9
Management of Companies and Enterprises	10
Manufacturing	11
Mining and Oil and Gas Extraction	12
Other Services (except Public Administration)	13
Professional, Scientific and Technical Services	14
Public Administration	15
Real Estate and Rental and Leasing	16
Retail Trade	17
Transportation and Warehousing	18
Utilities	19
Wholesale Trade	20
Other. Please specify: _____	21

53. What is your own position within the organization? (DO NOT READ LIST. ACCEPT ONE RESPONSE) T2011

Owner, President or CEO	1
General Manager/Other Manager	2
IT Manager	3
Administration	4
Vice President	5
Privacy analyst/officer/coordinator	6
Legal counsel/lawyer	7
HR/Operations	8
Other: Specify _____	9

54. In which of the following categories would your company's 2012 revenues fall? (READ LIST. ACCEPT ONE RESPONSE) T2011

Less than \$100,000	1
\$100,000 to just under \$250,000	2
\$250,000 to just under \$500,000	3



\$500,000 to just under \$1,000,000	4
\$1,000,000 to just under \$5,000,000	5
\$5,000,000 to just under \$10,000,000	6
\$10,000,000 to just under \$20,000,000	7
More than \$20 million	8

**This concludes the survey.**  
**Thank you for your time and feedback, it is much appreciated.**