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

Phoenix Strategic Perspectives Inc.

Final Report

2015 Public Opinion Research with Canadian Businesses on Privacy-Related Issues (telephone survey)

Prepared for Office of the
Privacy Commissioner of Canada

January 2016

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

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

Table of Contents

Executive Summary

The Office of the Privacy Commissioner of Canada (OPC) commissioned Phoenix Strategic Perspectives Inc. (Phoenix) to conduct quantitative and qualitative opinion research with Canadian businesses on privacy-related issues. The purpose of the research was to better understand: 1) the extent to which businesses are familiar with privacy issues and requirements; and 2) the types of privacy policies and practices that they have in place. This report presents the results of the 12-minute telephone survey administered to 1,016 companies across Canada. Data were collected December 1-18, 2015. Based on a sample of this size, the results can be considered accurate to within ±3.1%, 19 times out of 20.

Collection, Storage and Protection of Customer Information

Canadian businesses collect a variety of personal information about their customers. The vast majority of surveyed companies (93%) collect contact information, such as names, telephone numbers, and mailing or email addresses. Other types of customer information mentioned with some frequency include opinions, evaluations, and comments (27%), and financial information, such as invoices, credit cards, or banking records (25%). The type of customer information collected by companies has changed little since tracking began in 2011. Contact information, financial information and feedback continue to be the most frequently collected customer information.

Turning to storage methods, 62% of respondents said their business stores customer information on paper. As was the case in 2011 and 2013, paper was the top storage method. Following this, similar proportions store customer information on desktop computers (54%) and on-site servers (53%). Roughly one-quarter (24%) said their business stores this type of information on portable devices, such as laptops, USB sticks, or tablets. Seventeen percent store customer information electronically through cloud computing, and 11% store such information with a third party service other than cloud computing (such as a documentation warehouse). Since 2013, the use of on-site servers for data storage has decreased from 58% to 53%, while the percentage of companies storing data via cloud computing has increased from 7% to 17%.

Ninety-three percent of the businesses surveyed use at least one security method to protect their customers' personal information and exactly half employ four to five measures. Passwords (79%) are the most common, followed by physical methods (74%), such as locked filing cabinets, restricting access, and security alarms. Smaller proportions use firewalls (65%) and organizational controls (63%), such as security policies and procedures. One in three respondents (32%) said their business employs encryption to protect customer personal information. Over time, the use of technological tools (passwords, firewalls, or encryption) has increased, from 78% in 2013 to 83% in 2015. Conversely, the use of physical measures has decreased, from 78% in 2013 to 74% in 2015.

Company Privacy Practices

Two-thirds of business executives surveyed (67%; down from 70% in 2013) said their company attributes high importance to protecting customer personal information. Only

11% indicated that protecting customers' personal information is not an important objective for their company.

Business representatives were asked whether they had in place a series of privacy practices. Underscoring the importance companies attribute to protecting customers' personal information, half or more of the surveyed businesses have a designated privacy officer (57%), internal policies for staff that address privacy obligations (50%), and procedures for dealing with customer complaints (50%). Forty-four percent have a privacy policy that explains to customers how they will collect and use customer personal information. Companies were least likely to regularly provide staff with privacy training and education (32%). On average, businesses employ three (2.78) of these personal information-handling practices. Among the practices that have been tracked, the proportion of companies implementing them has changed very little.

Managing Privacy Risks

While the majority of companies consider privacy a highly important objective, just 37% of business executives said their company has policies or procedures to assess privacy risks related to business (up from 28% in 2013). This includes assessing privacy risks associated with the development or use of new products, services, or technologies.

This survey also examined companies' rate of adopting practices that may increase risks to personal information, including third party data management and allowing employees to use personal devices for company purposes. It also asked respondents about their concerns about and means of dealing with a data breach.

Fewer than one in five (17%) companies send customer information to a third party for processing or storage, which may include the use of cloud computing.[1] This represents a modest increase of five percentage points since 2013, when 13% of businesses sent information to a third party.

Business representatives were also asked about their company's policy on allowing employees to use their personal electronic devices, such as smartphones, tablets or laptops, for work purposes. Nearly one in four companies (23%) companies allow employees to use personal electronic devices for work purposes.

Executives were divided on how concerned they are about a data breach where their customers' personal information is compromised. Roughly one-quarter (26%) provided the highest rating of *extremely* concerned, whereas slightly more (30%) said they are not concerned at all. Overall, 32% of respondents expressed high concern, 23% moderate concern, and 44% low or no concern. Over time, the proportion of executives at least somewhat concerned about a data breach has increased from 41% in 2013 to 48% in 2015.

A strong minority (41%) of surveyed companies have policies or procedures in place to be followed in the event of a breach where customer personal information is compromised. This represents a small increase since 2013, when 37% reported having guidelines for

[1] Earlier in the survey, respondents were asked how their company stores customer information. Multiple responses were accepted, including cloud computing. This question focused specifically on the use of third parties for any type of service, including storage.

responding to a breach. Conversely, just over half (55%) of the business executives surveyed said their company does not have procedures in place (5% were uncertain whether or not their business has protocols).

Awareness and Impact of Federal Privacy Law

Business executives were asked to rate their company's awareness of its responsibilities under Canada's privacy laws. A strong minority (43%) think their company is highly aware of its responsibilities. A slightly smaller proportion (39%) indicated that their company has a moderate level of familiarity with their privacy responsibilities. In total, 82% of companies are at least somewhat familiar their responsibilities under Canada's privacy laws. While the proportion of respondents who said their company is highly aware of its responsibilities under Canada's privacy laws is virtually unchanged since 2013, it remains lower than it was when the baseline survey was conducted in 2007. At that time, roughly half (49%) of the executives surveyed said their company is highly aware of its privacy obligations.

Executives were asked to rate their level of awareness of the Personal Information Protection and Electronics Document Act (PIPEDA), Canada's federal private-sector privacy law. In total, 37% said their company is highly aware of the legislation, while 40% rated their company as moderately aware. In total, 77% of companies are at least somewhat familiar with PIPEDA. Overall, awareness of PIPEDA increased slightly from 2013 to 2015, which establishes a positive trend with the number of companies with high awareness increasing from 27% in 2011 to 37% in 2015.

A small majority of business executives (59%) said their company has taken steps to ensure that it complies with PIPEDA. Nearly nine in 10 (89%) of the companies that have taken steps to comply with Canada's federal privacy legislation (n=657) found compliance to not be difficult. The small number of executives who said it was difficult for their company to comply (n=56) provided a variety of reasons to explain why. The following reasons were offered with the greatest frequency: lack of understanding of the legislation (17%); lack of up to date knowledge (14%); and the cost of complying (13%).

Communications and Outreach

Business executives were asked which organizations or resources their company uses to help clarify its responsibilities under Canada's privacy laws. Almost half the executives surveyed (45%) said their company does not consult any resources for help with compliance. Among companies that have sought assistance (n=628), the top resource identified was the Internet (42%). Following the Internet, 25% consult provincial or federal government organizations, including the federal privacy commissioner (which was cited by 8% of executives).

A strong minority (41%) of surveyed business executives were aware that the OPC has information and tools to help companies comply with their privacy obligations. Awareness is virtually unchanged since 2011, when it dropped to 40% from a high of 55% in 2010.

Subgroup Differences

Business size is the strongest and most consistent predictor of a company's privacy practices. Larger businesses (with at least 100 employees) tend to employ more methods

of protecting customer information, and are more likely to have risk assessment policies or procedures in place. Larger companies are also more likely to place a higher amount of importance on protecting privacy, to have a higher awareness of PIPEDA, and to have taken steps to ensure compliance with the federal privacy legislation.

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

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

Introduction

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

Background and Objectives

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

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

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

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

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

Research Design

To meet the research objectives, quantitative and qualitative research were conducted with Canadian businesses. The focus of this report is the quantitative component of the study. A 12-minute telephone survey was administered to 1,016 companies across Canada, stratified by business size. 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. Based on a sample of this size, the results can be considered accurate to within ±3.1%, 19 times out of 20.

The following specifications applied to the survey:

- The target respondents were senior decision makers 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 for each of the three target business size quotas: small (one-19 employees); medium (20-99 employees; and large (100+ employees).
- A telephone pre-test was conducted in English and French, with 10 interviews in each official language. Interviews were digitally recorded for review afterwards.
- Interviews were conducted in the respondent's official language of choice.
- The survey was registered with Marketing Research and Intelligence Association's (MRIA) national survey registration system.
- Respondents were informed that the survey was commissioned by OPC.
- Data were collected December 1-18, 2015.

The following table presents information about the final call dispositions for this survey, as well as the associated response rate (using the MRIA formula)[3]:

Total Numbers Attempted	**9,213**
Out-of-scope - Invalid	**1,045**
Unresolved (U)	**3,075**
No answer/Answering machine	3,075
In-scope - Non-responding (IS)	**4,055**
Language barrier	22
Incapable of completing (ill/deceased)	4
Callback (Respondent not available)	3,053
Refusal	912
Termination	64
In-scope - Responding units (R)	**1,038**
Completed Interview	1,016
NQ - Quota Full - Company Size	22
Response Rate	**12.7%**

Notes to Readers

- Reference is made to findings from similar surveys conducted for the OPC with Canadian businesses in 2007, 2010, 2011 and 2013. 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.

[3] 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].

- 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.
- The survey questionnaire is appended to the report.

Collection, Storage and Protection of Customer Information

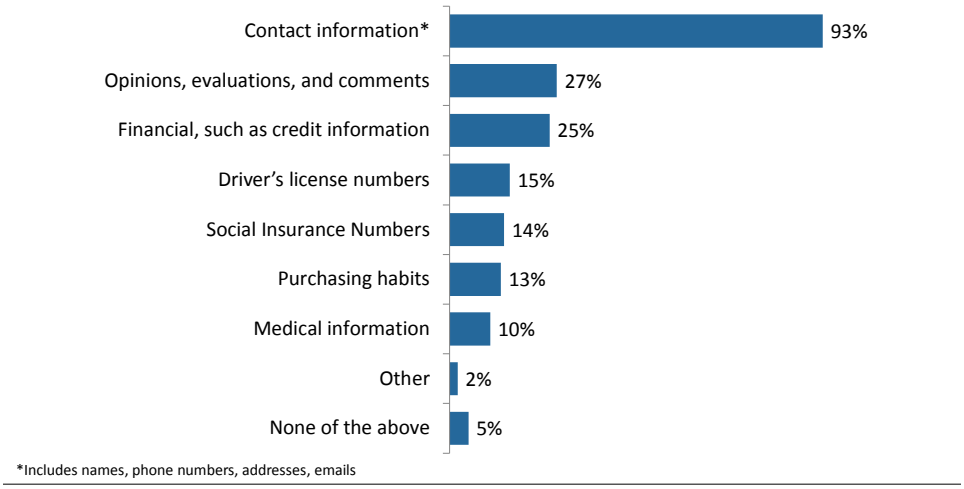
This section identifies the type of customer personal information collected by businesses, how the data is stored, and the measures taken by companies to protect it from disclosure.

Contact Information—Most Widely Collected Customer Information

In terms of the types of information collected about customers, the vast majority of surveyed companies (93%) collect contact information, such as names, telephone numbers, and mailing or email addresses. Other types of information mentioned with some frequency include opinions, evaluations, and comments (27%), and financial information, such as invoices, credit cards, or banking records (25%).

As the graph depicts, other types of information are collected about customers by smaller proportions of businesses.

Type of Customer Information Collected



Q3. Which of the following types of information does your company collect about your customers? Multiple responses accepted

Base: n=1,016; all respondents

In total, 5% of respondents said their company does not collect any of these types of customer information.

The type of customer information collected by companies has changed little since tracking began in 2011. Contact information, financial information and feedback continue to be the most frequently collected customer information.

Subgroup Findings:

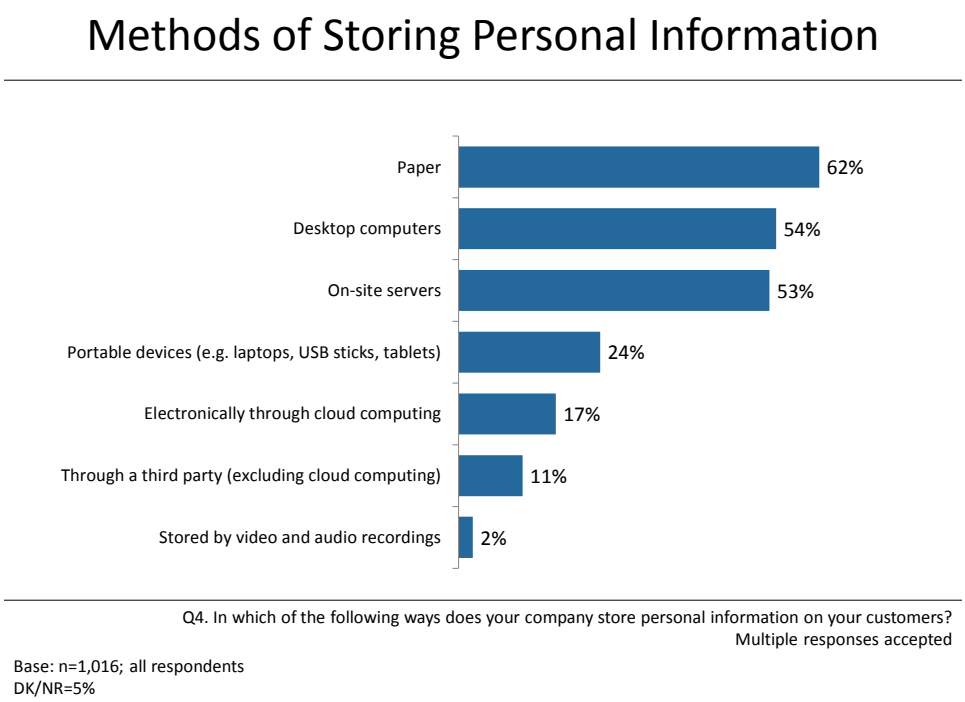
Larger businesses collect more information about their customers. Companies with 100 employees or more collect 2.8 different types of information on average (versus 2.0 to 2.2 for companies with fewer than 100 employees).

With respect to sector, businesses operating in the financial sector collect significantly more personal information from customers: on average, 3.4 different types of information compared to two or fewer by companies active in other sectors. Specifically, companies in the financial sector were more likely to collect financial information (61% vs. 12% to 28% in other sectors), driver's license numbers (52% vs. 1% to 20%), and social insurance numbers (58% vs. 3% to 13%) from customers.

Variety of Methods Used to Store Personal Information—Primarily On-Site

Businesses use a variety of methods to store customers' personal information, with the vast majority storing it on-site. Just under two-thirds (62%) of respondents said their business stores customer information on paper. As was the case in 2011 and 2013, on-site on paper was the top method used by businesses. Following this, similar proportions store customer information on desktop computers (54%) and on-site servers (53%).

Roughly one-quarter (24%) said their business stores this type of information on portable devices, such as laptops, USB sticks, or tablets. Seventeen percent store customer information electronically through cloud computing, and 11% store such information with a third party.



Q4. In which of the following ways does your company store personal information on your customers?
Multiple responses accepted

Base: n=1,016; all respondents
DK/NR=5%

Since 2013, the use of on-site servers for data storage has decreased from 58% to 53%, while the percentage of companies storing data via cloud computing increased from 7% to 17%.

Subgroup Finding:

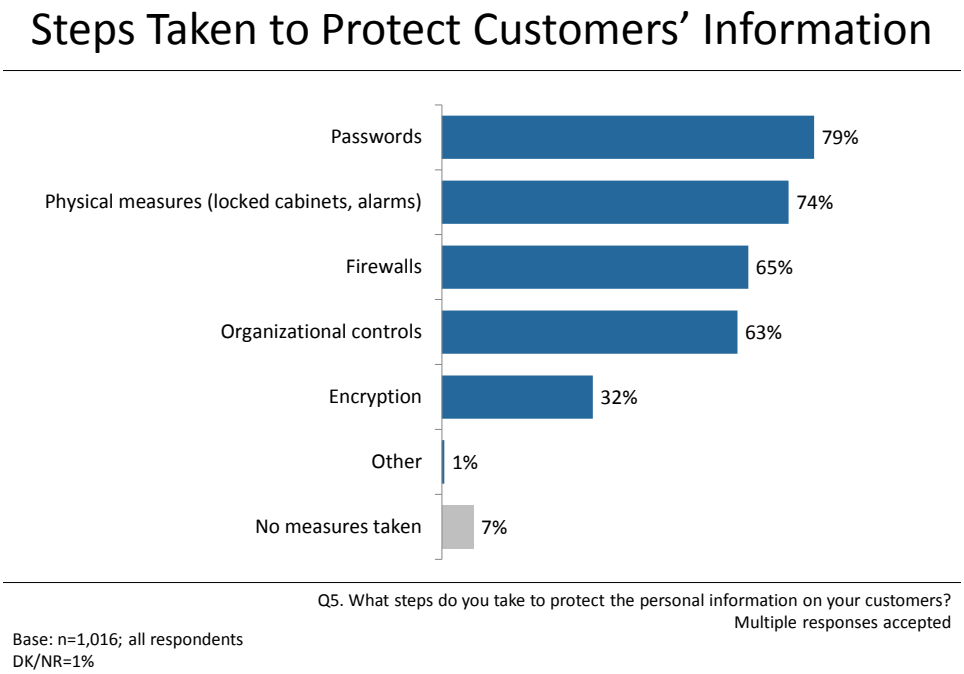
Large businesses are more likely to store information on on-site servers, and are less likely to store information directly on desktop computers.

Electronic and Physical Measures Taken to Protect Personal Information

The vast majority of Canadian businesses (93%) use at least one security method to protect the personal information of their customers. Moreover, businesses tend to employ more than one measure, with exactly half of the respondents saying their business uses four to five measures.

Passwords are the most common security measure, but only by a small margin of five percentage points. Roughly four in five (79%) businesses use passwords. Following closely at 74% are physical methods, such as locked filing cabinets, restricting access, and security alarms. Smaller proportions use firewalls (65%) and organizational controls (63%), such as security policies and procedures.

Only one in three survey respondents (32%) said their business employs encryption to protect customer personal information.



Over time, the use of technological tools (passwords, firewalls, or encryption) to protect customer information has increased five percentage points, from 78% in 2013 to 83% in 2015. Conversely, the use of physical measures has decreased four percentage points since 2013, from 78% to 74% in 2015.

Subgroup Findings:

Businesses tend to employ more means of protecting customer information as they increase in size: self-employed individuals use an average of two (2.3) methods of protecting customer information, companies with 2 to 19 employees use three (3.2), companies with 20 to 99 employees use more than three (3.6), and large business use more than four (4.3) methods on average. Accordingly, 19% of sole proprietorships have not taken measures to protect customer information, versus 1% to 6% of larger companies.

Businesses based in Atlantic Canada and Quebec tend to employ fewer methods of protecting customer information than those in other regions, and businesses based in Atlantic Canada are more likely than businesses in other regions to employ *no* measure at all to protect customers' personal information.

Businesses were particularly likely to use *more* methods of protecting information if they operate in the finance (4.0 on average), manufacturing (3.8), or health sectors (3.4).

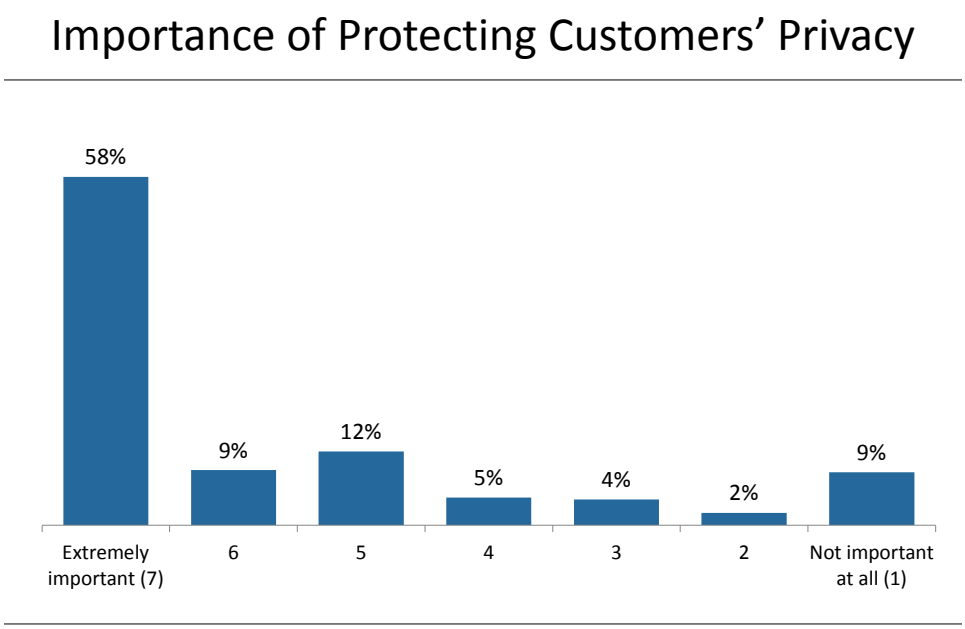
Company Privacy Practices

This section identifies the procedures and policies companies have in place to protect the personal information they collect about their customers.

Most Attribute High Importance to Protecting Customers' Privacy

Most business executives said their company attributes significant importance to privacy protection. A small majority (58%) chose the highest score available (on a 7-point scale), indicating their belief that protecting customers' personal information is an *extremely* important corporate objective. In total, two-thirds said that protecting customers' privacy is of *high* importance (scores of six to seven). The rest (21%) were more likely to attribute moderate importance to this (scores of three to five).

Only 11% of executives indicated that protecting customers' personal information is not an important objective for their company.

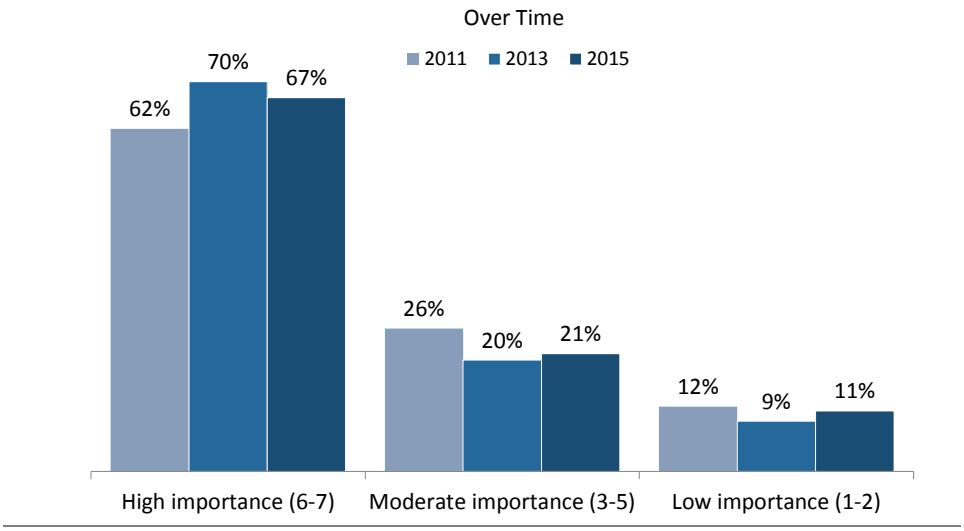


Base: n=1,016; all respondents
DK/NR=1%

Q12. What importance does your company attribute to protecting your customers' personal information?

Compared to 2013, the proportion of businesses that attribute a high level (scores of six or seven) of importance to protecting customers' personal information decreased three percentage points from 70% to 67%.

Importance of Protecting Customers' Privacy



Base: all respondents; DK/NR=1-6%
2011: N=1,006
2013: n=1,006
2015: n=1,016

Q12. What importance does your company attribute to protecting your customers' personal information?

Subgroup Findings:

Businesses are more likely to attribute high importance to protecting their customers' personal information if they sell to consumers (67% of those that sell to *both* consumers and business and 74% of those that sell only to consumers vs. 56% of those that sell only to businesses), and if they are larger in terms of employee size (83% of businesses with 100 or more employees vs. 59% of sole proprietorships to 72% of companies employing five to nine employees).

The importance that a business attributes to protecting the customers' personal information also increases as a function of the type of information they collect about their customers. For example, businesses are more likely to attribute *high* importance to protecting customers' information if they collect medical information (85%), social insurance numbers (86%), or financial information (81%). Conversely, businesses are less likely to attribute *high* importance to protecting customers' information if they collect other information, such as customers' names and phone numbers (68%) or purchasing habits (70%).

Companies that operate in the finance sector are more likely to attribute high importance to protecting customers' information than companies active in other sectors of the economy (85% vs. 50% to 76% in other sectors).

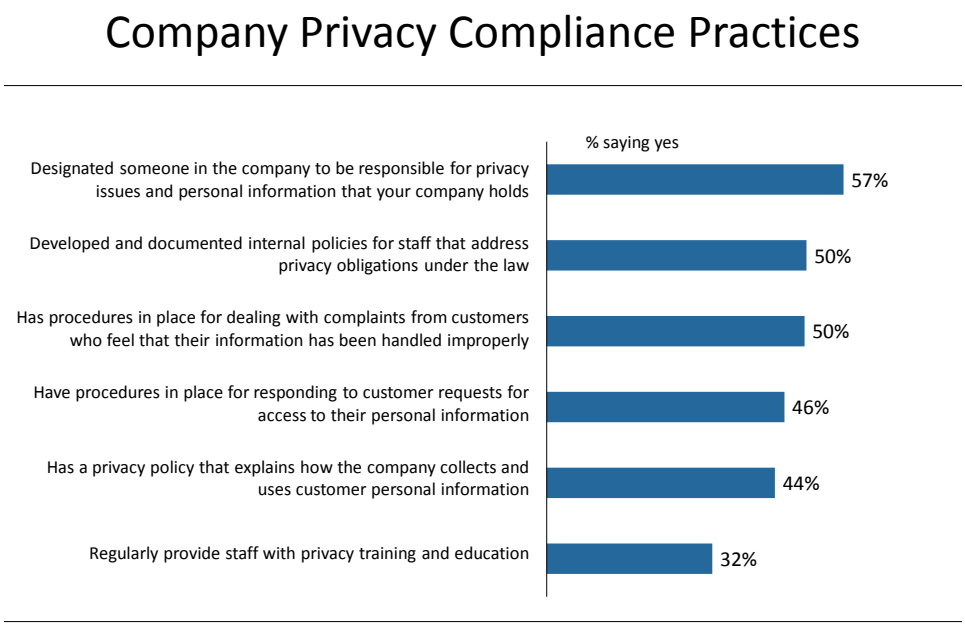
Uneven Implementation of Privacy Compliance Practices

Business representatives were asked whether they had in place a series of privacy practices. These 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.

Half or more of surveyed businesses have put in place three of these practices. This includes having a designated privacy officer (57%), internal policies for staff that address privacy obligations (50%), and procedures for dealing with customer complaints (50%). Companies were least likely to regularly provide staff with privacy training and education. Approximately one-third (32%) of respondents said their business provides this type of staff training and education.

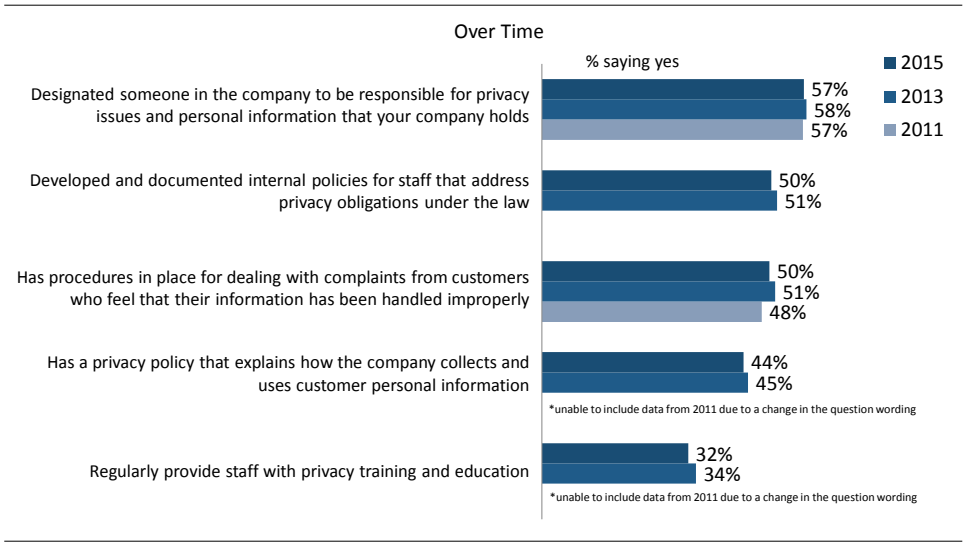
On average, businesses employ three (2.78) of these personal information-handling practices. At the high end, 28% of businesses have implemented five or all of the practices; conversely, one in five surveyed businesses have put in place none of these privacy-related mechanisms.



Base: n=1,016; all respondents
DK/NR=1-6%

Among the practices that have been tracked, the proportion of companies implementing them has changed very little.

Company Privacy Compliance Practices



Base: all respondents; 2011: n=1,006, 2013: n=1,006, 2015: n=1,016

Subgroup Findings:

Overall, the strongest determinant of how many of these privacy-related practices a business has adopted is how many different types of information they collect from their customers. For example, companies that collect only one type of personal information have implemented, on average, two (2.0) of these practices. In contrast, businesses that reportedly collect five types of personal information from their customers have adopted, on average, four (4.4) of these practices.

Companies were also more likely to have implemented more of these privacy-related practices if they operate in the health or finance sectors. For example, 73% of businesses active in the health sector, and 71% of businesses in the finance sector, have designated an individual to be responsible for privacy issues. Far fewer (45% to 58%) of businesses operating in other sectors reported having done so.

The likelihood of having adopted more of these policies was higher among the following types of companies: those with revenues over $20 million, those that sell *only* to consumers rather than *only* to businesses, and those that are based outside of Quebec.

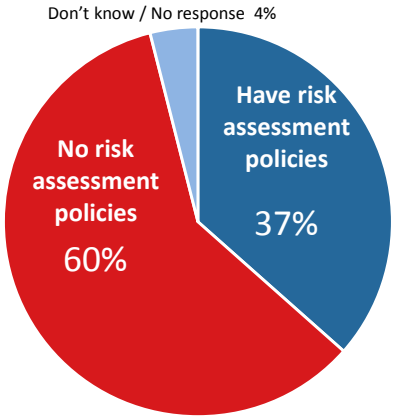
Managing Privacy Risks

This section looks at companies' rate of adopting process to assess privacy risks along with their rate of adopting practices that may increase risks to personal information, including third party data management and allowing employees to use personal communication devices for company purposes. It also examines respondents' level of concerns about and plans for dealing with data breaches.

More than One-Third Have Policies in Place to Assess Privacy Risks

More than one-third (37%) of business executives said their company has policies or procedures to assess privacy risks related to business. This includes assessing privacy risks associated with the development or use of new products, services, or technologies. This represents an increase of nine percentage points since 2013, when 28% of companies reported having such policies or procedures.

Policies in Place to Assess Privacy Risks



Q20. 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.

Base: n=1,016; all respondents

Subgroup Findings:

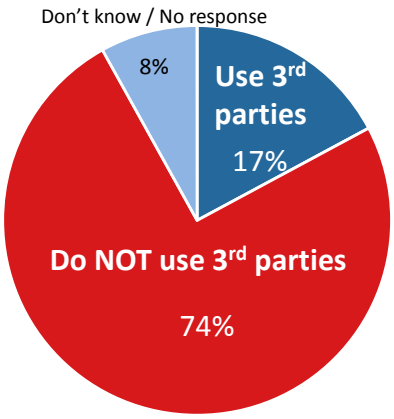
Companies that collect more types of personal information about their customers are more likely to have established policies or procedures to assess risks related to their business. For example, 69% of companies that collect five or more types of information (e.g., contact, financial, medical, SINs) have established risk assessment policies or procedures, whereas 34% of companies that collect one to three types have established such policies or procedures.

Businesses with 100 or more employees were more likely to have risk assessment policies or procedures in place (66% vs. 31% to 41% of smaller businesses).

Few Companies Use Third Parties to Manage Customer Information

Fewer than one in five (17%) send customer information to a third party for processing or storage, which may include the use of cloud computing.[4] This represents a modest increase of five percentage points since 2013, when 13% of businesses sent information to a third party.

Use of Third Parties to Manage Personal Information



Base: n=1,016; all respondents

Q21. 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?

Subgroup Finding:

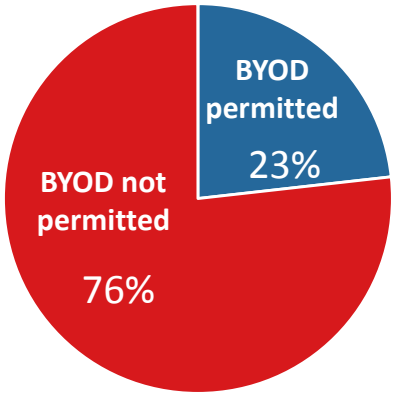
Companies that sell *only* to other businesses were the more likely to use third parties (24% vs. 14%-15% of those that sell to consumers or ***both*** customers and businesses).

Minority of Companies Allow Employees to Use Personal Devices for Work

Business representatives were asked about their company's stance on "Bring Your Own Device" (BYOD), where employees may be allowed to use their personal electronic devices, such as smartphones, tablets or laptops, for work purposes. Nearly one in four companies (23%) companies allow employees to use personal electronic devices for company work.[5] Conversely, the majority of companies surveyed (76%) do not allow this practice.

[4] Earlier in the survey, respondents were asked how their company stores customer information. Multiple responses were accepted, including cloud computing. This question focused specifically on the use of third parties for any type of service, including storage.
[5] Tracking data is not available for this question, as the wording was changed from the 2013 survey.

Use of Non-Company-Issued Electronic Devices



Base: n=1,016; all respondents
DK/NR: <1%

Q22. Does your company allow employees to use personal electronic devices, such as smartphones, tablets, PCs, or other electronic devices, for work purposes, such as accessing company networks or data?

Subgroup Finding:

Businesses were more likely to allow their employees to use their personal electronic devices for work purposes if they employed 100 people or more (46% vs. 19%-28%), or if they were based in the Greater Toronto Area (33% vs. 13%-20% of other regions).

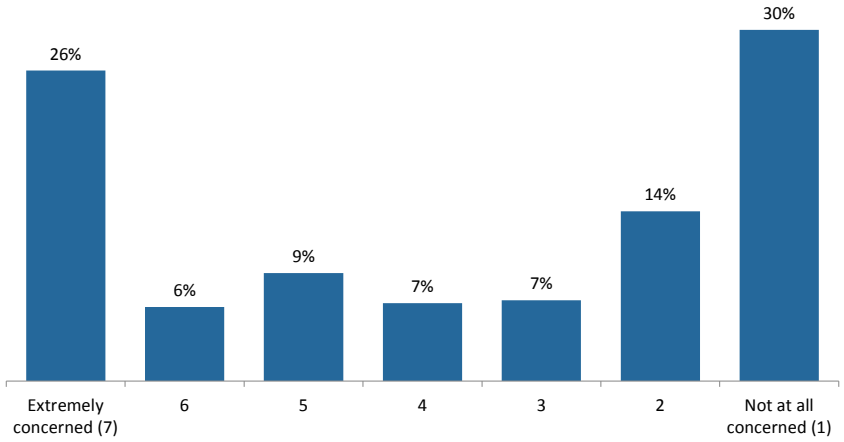
Businesses Split on Concern Over Data Breach

Surveyed executives were divided on how concerned they are about a data breach where their customers' personal information is compromised. Roughly one-quarter (26%) provided the highest rating of *extremely* concerned (seven out of seven), whereas slightly more (30%) said they are not concerned at all. Overall, 32% of respondents expressed high concern (six or seven out of seven), 23% moderate concern (three to five), and 44% low or no concern (one or two).

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.*

Concern about a Data Breach

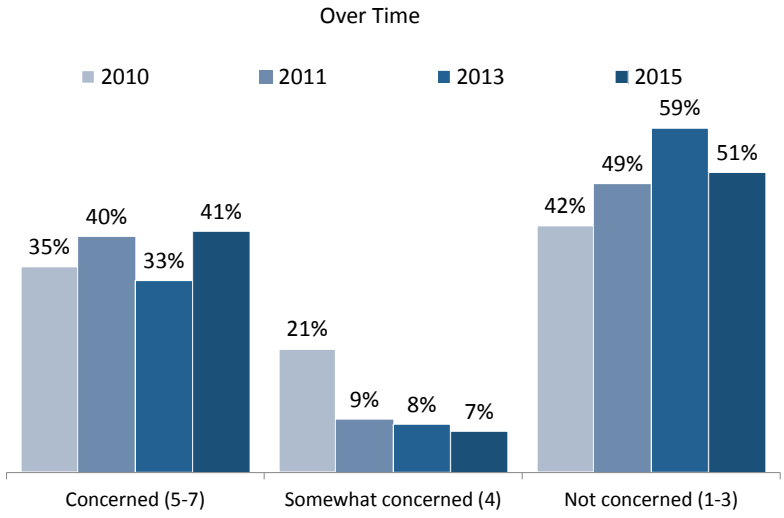


Base: n=1,016; all respondents
DK/NR=1%

Q18. How concerned are you about a data breach, where the personal information of your customers is compromised?

Levels of concern about a data breach have increased from 2013, with the proportion of executives concerned (five to seven out of seven) about a data breach having gone up eight percentage points, accompanied by a drop in the proportion saying they are not concerned.

Concern about a Data Breach

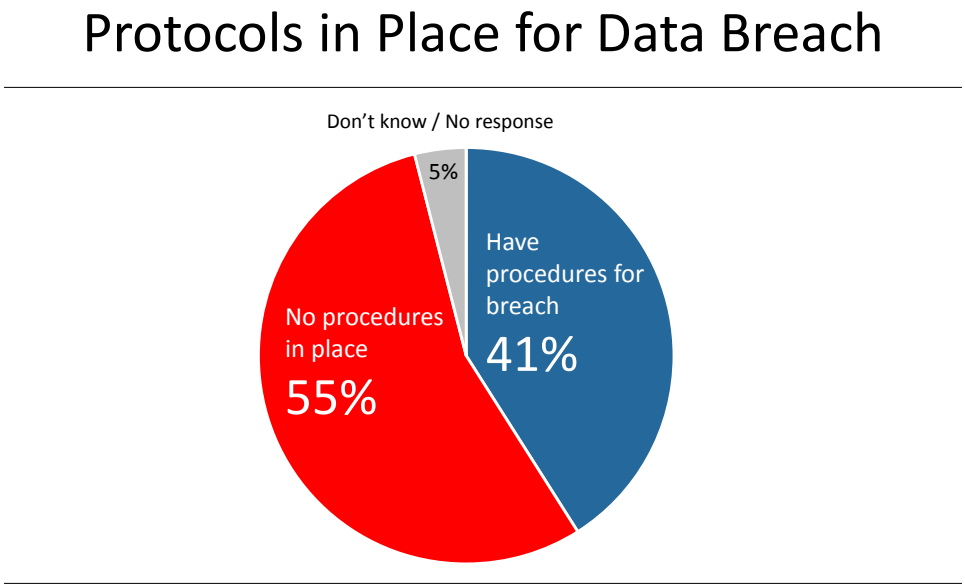


Base: all respondents; 2011: n=1,006
2013: n=1,006, 2015: n=1,016
DK/NR=1%-2%

Q18. How concerned are you about a data breach, where the personal information of your customers is compromised?

Strong Minority Have Protocols for Data Breach

A strong minority (41%) of surveyed companies have policies or procedures in place to be followed in the event of a breach where customer personal information is compromised. Conversely, just over half (55%) of the business executives surveyed said their company does not have procedures in place (5% were uncertain whether or not their business has protocols).



Q19. 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?

Base: n=1,016; all respondents

This represents a small increase since 2013, when 37% reported having guidelines for responding to a breach, and a significant increase since 2011 when 31% of surveyed companies had protocols in place.[6]

[6] 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.

Subgroup Findings:

Companies expressed a higher level of concern over a data breach if they collected more types of personal information about their customers. More than half (57%) of representatives of companies that collect between five and seven types of information expressed *high* concern about a data breach compared to three in ten of surveyed executives whose company collects three or fewer pieces of personal information from customers.

Representatives of businesses based in Quebec were substantially more likely to express high levels of concern about a data breach, with 50% rating their concern as six or seven on the seven-point scale compared to 27% to 33% of executives whose companies were based in other regions.

With respect to preparedness to respond to a data breach, the likelihood of having protocols in place was lower among: companies based in Atlantic Canada (26%), Quebec (29%) or the prairies (36%) compared to companies elsewhere in the country; and companies with fewer than 100 employees (32% of self-employed individuals to 49% of companies employing five to nine staff vs. 63% of businesses with 100 employees or more).

Awareness and Impact of Federal Privacy Law

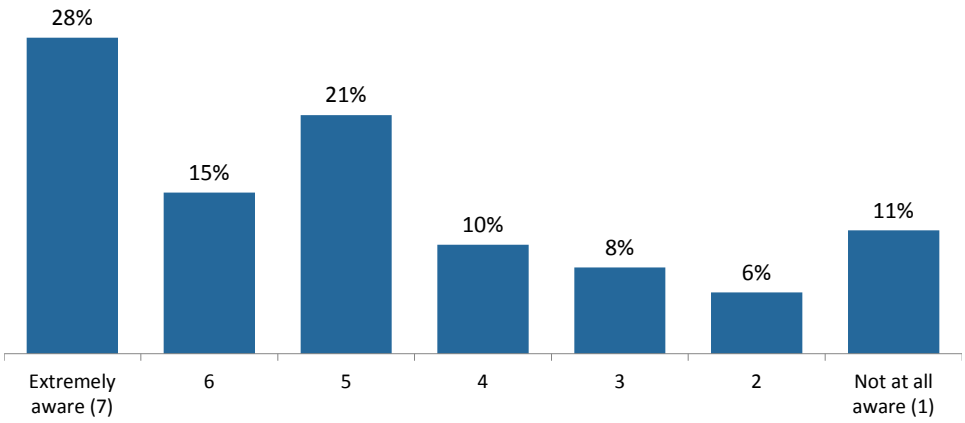
This section presents findings regarding companies' awareness of their responsibilities under privacy laws. Questions in this section were prefaced with the following description of Canada's privacy laws:

> *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.*

Modest Level of Awareness of Responsibilities under Privacy Laws

Business executives were asked to rate their company's awareness of its responsibilities under Canada's privacy laws. A strong minority (43%) think their company is highly aware of its responsibilities (scores six or seven on the scale), with 28% selecting the highest rating of *extremely aware*. A slightly smaller proportion indicated that their company has a moderate level of familiarity with their privacy responsibilities (scores of three to five). Fewer than one in five (17%) rated their company's awareness as low (score of one to two).

Company's Awareness of Responsibilities under Privacy Laws

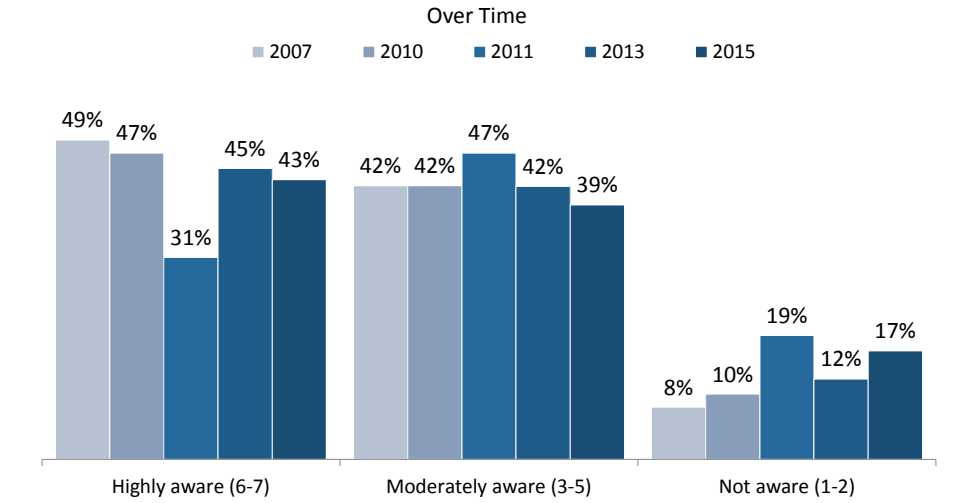


Q13. How would you rate your company's awareness of its responsibilities under Canada's privacy laws?

Base: n=1,016; all respondents
DK/NR=3%

Compared to 2013, there has been a small, but notable, increase in the proportion of executives that rated their company's awareness as low (from 12% in 2013 to 17% in 2015). While the proportion of respondents who said their company is highly aware of its responsibilities under Canada's privacy laws is virtually unchanged since 2013, it remains lower than it was when the baseline survey was conducted in 2007. At that time, roughly half (49%) of the executives surveyed said their company is highly aware of its privacy obligations.

Company's Awareness of Responsibilities under Privacy Laws



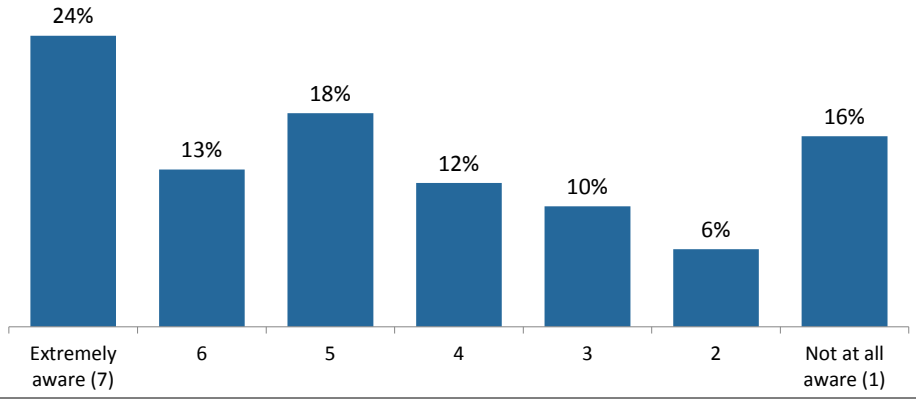
Base: all respondents; 2011: n=1,006, 2013: n=1,006, 2015: n=1,016
DK/NR=1-3%

Q13. How would you rate your company's awareness of its responsibilities under Canada's privacy laws?

Executives Report More Limited Awareness of PIPEDA

Executives were also asked to rate their level of awareness of PIPEDA. In total, 37% said their company is *highly* aware (scores of six or seven on the seven-point scale) of the legislation. Four in 10 rated their company as moderately aware of PIPEDA (scores of three to five), while roughly one in five (22%) characterized their company as having low awareness or none at all (score of one or two).

Company's Awareness of PIPEDA



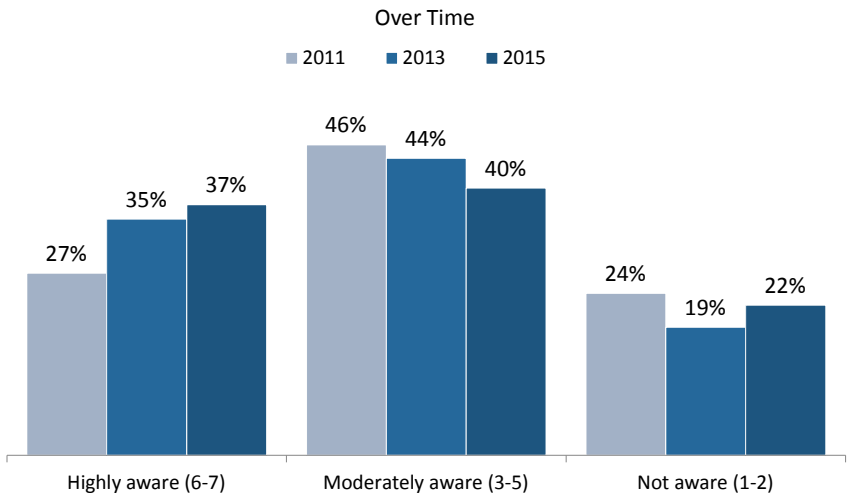
Q14. Thinking specifically about PIPEDA, the federal government's privacy law, how would you rate your company's awareness of this legislation?

Base: n=1,016; all respondents
DK/NR=2%

Awareness of PIPEDA specifically is therefore slightly lower than awareness of responsibilities under Canada's privacy laws more generally.

The number of companies with high awareness of PIPEDA has increased from 27% in 2011 to 37% in 2015.

Company's Awareness of PIPEDA



Base: all respondents; 2011: n=1,006, 2013: n=1,006, 2015: n=1,016
DK/NR=1-3%

Q14. Thinking specifically about PIPEDA, the federal government's privacy law, how would you rate your company's awareness of this legislation?

Subgroup Findings:

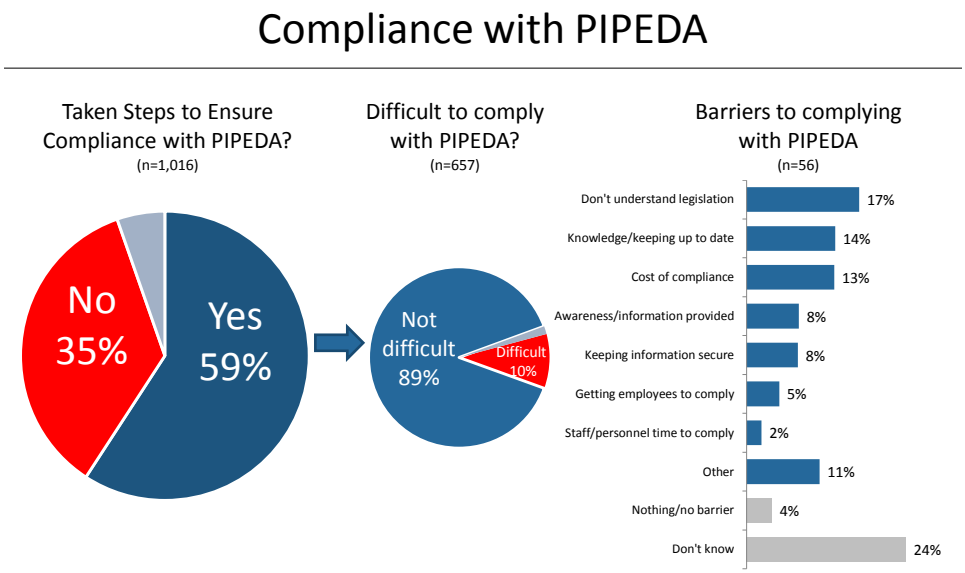
Business executives were more likely to rate their company's awareness of its responsibilities under Canada's privacy laws highly if the company has 100 employees or more (69% vs. a high of 45% of smaller companies). Among companies with only a single employee, 26% said they were not at all aware of their privacy responsibilities compared to a high of 12% of larger companies.

Similarly, awareness of their privacy responsibilities was higher among companies that collect more types of information about their customers. In total, 70% of companies that collect five to seven types were characterized as having a high level of awareness versus 40% of those that collect three or fewer pieces of information. Awareness of their privacy responsibilities was higher among companies that operate in the finance (68%) or health (61%) sectors.

Awareness of PIPEDA specifically was higher among larger companies and those based in the Greater Toronto Area and Quebec. In addition, companies that sell *only* to consumers were more likely to be highly aware of PIPEDA (41% highly aware vs. 34% of companies selling to businesses). Finally, awareness of PIPEDA was higher among companies that operate in the health (61%) or finance (58%) sectors.

Small Majority Have Taken Steps to Comply with PIPEDA

A small majority of business executives (59%) said their company has taken steps to ensure that it complies with PIPEDA. Nearly nine in 10 (89%) of the companies that have taken steps to comply with Canada's federal privacy legislation (n=657) found compliance to not be difficult.



[Left] Q15. Still thinking specifically about PIPEDA, has your company taken steps to ensure that it complies with the federal government's privacy law?
[Middle] Q16: Was it difficult for your company to comply with PIPEDA?
[Right] Q17: In your view, what was the most significant barrier or challenge for your company in terms of complying with PIPEDA?

The small number of executives who said it was difficult for their company to comply (n=56) provided a variety of reasons to explain why. The following reasons were offered with the greatest frequency: lack of understanding of the legislation (17%); lack of up to

date knowledge (14%); and the cost of complying (13%). Almost one-quarter (24%) did not know why it was difficult.

Subgroup Findings:

Companies were more likely to have taken steps to ensure compliance with PIPEDA if they sell to consumers ***only*** (65%) or ***both*** consumers and businesses (60%), have 100 employees or more (82%), operate in core industries[7] (64%), or are active in the health sector (84%). With respect to the ease of complying with PIPEDA, businesses based in British Columbia were somewhat more likely to describe the process as difficult (19%).

[7] 'Core' industries are industries that would be expected to collect customer personal information more than other industries (i.e., industries for whom privacy laws have greater relevance). The table in Annex 1 details how subgroup characteristics have been grouped for the analysis.

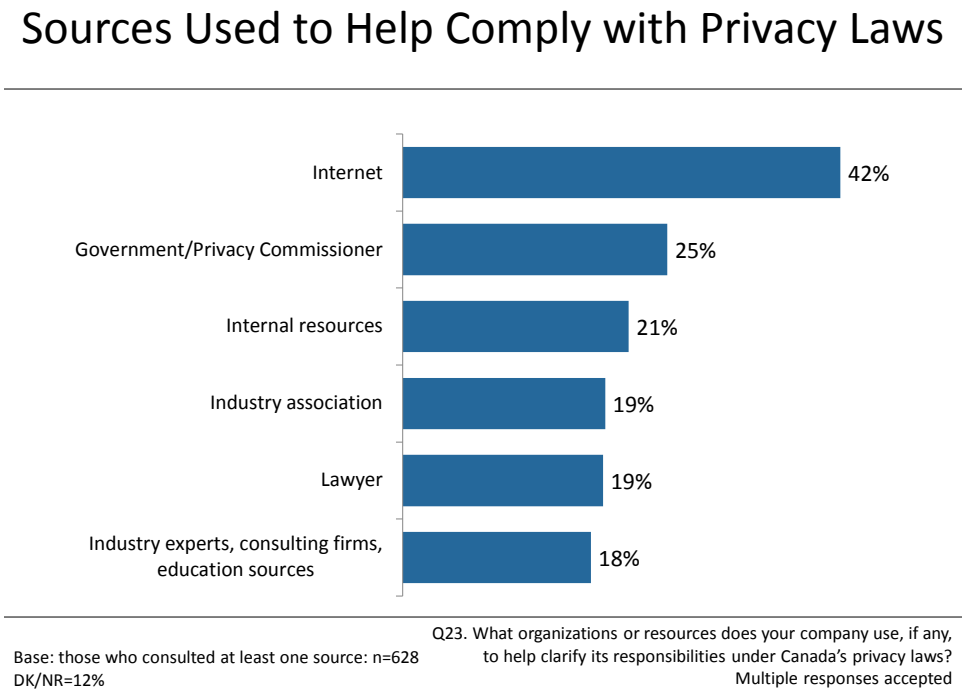
Communications and Outreach

This section presents executives' feedback on the sources their companies use to gather information relating to privacy issues, as well as awareness of resources available from the Office of the Privacy Commissioner of Canada (OPC).

Internet—Top Source for Privacy Law Compliance Information

Business executives were asked which organizations or resources their company uses to help clarify its responsibilities under Canada's privacy laws. Almost half the executives surveyed (45%) said their company does not consult any resources for help with compliance.

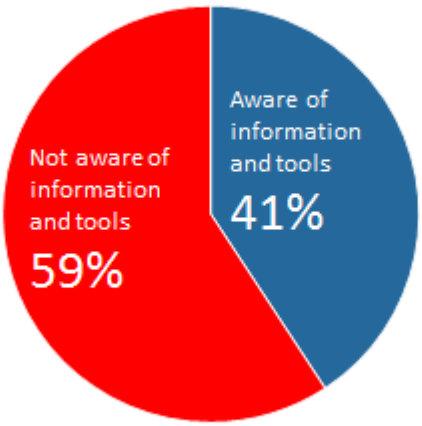
Among companies that have sought assistance (n=628), the top resource identified was the Internet (42%). Following the Internet, 25% consult provincial or federal government organizations, including the federal privacy commissioner (which was cited by 8% of executives).



Strong Minority Aware of Resources Provided by the OPC

Roughly two in five (41%) surveyed business executives were aware that the OPC has information and tools to help companies comply with their privacy obligations. Conversely, 59% said they were not aware of such resources. Awareness is virtually unchanged since 2011, when it dropped to 40% from a high of 55% in 2010.

Awareness of OPC Resources



Q19. 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?

Base: n=1,016; all respondents
DK/NR = <1%

Subgroup Findings:

Representatives were least likely to be aware that the OPC has information and tools available to help companies comply with privacy obligations if they were based in Quebec (26%). Awareness was also higher among companies with ten employees or more (from 44% to a high of 51% of the largest companies).

Corporate Profile

The following tables present the characteristics of survey respondents (using weighted data).

Customer Type	Percent
Sells directly to consumers	36%
Sells directly to other businesses/organizations	25%
Sells directly to consumers and other businesses/organizations	37%
Is a government organization	1%
Other	1%

Region	Percent
Atlantic Canada	6%
Quebec	21%
Manitoba and Saskatchewan	7%
Alberta	14%
British Columbia	16%
Ontario (excluding the Greater Toronto Area)	19%
Greater Toronto Area	17%

Business Size	Percent*
Self-employed (1 employee)	16%
Small (2-19 employees)	70%
Medium (20-99 employees)	10%
Large (100+ employees)	2%
Don't know / no response	1%

Language of interview	Percent
English	81%
French	19%

Revenues in 2014	Percent*
Less than $100,000	17%
$100,000 to just under $250,000	15%
$250,000 to just under $500,000	9%
$500,000 to just under $1,000,000	10%
$1,000,000 to just under $5,000,000	21%
$5,000,000 to just under $10,000,000	3%
$10,000,000 to just under $20,000,000	2%
More than $20 million	2%
Don't know / no response	20%

*Percentages do not sum to 100% due to rounding error.

Appendix

Annex 1: Subgroup Categories

Core Industries[8]*:* ◦ Accommodation and Food Services ◦ Administrative & Support, Waste Management and Remediation Services ◦ Arts, Entertainment and Recreation ◦ Educational Services ◦ Finance and Insurance ◦ Health Care and Social Assistance ◦ Information and Cultural Industries ◦ Professional, Scientific, Technical Services ◦ Public Administration ◦ Real Estate and Rental and Leasing ◦ Retail Trade ◦ Transportation and Warehousing ◦ Utilities ◦ *Non-Core Industries*: ◦ Agriculture, Forestry, Fishing and Hunting ◦ Construction ◦ Management of Companies, Enterprises ◦ Manufacturing ◦ Mining and Oil and Gas Extraction ◦ Other Services (except Public Admin.) ◦ Wholesale Trade ◦ Other *Revenues* ◦ Less than $1,000,000 ◦ $1,000,000 to just under $10,000,000 ◦ $10,000,000 to just under $20,000,000 ◦ More than $20 million *Region*: ◦ Quebec ◦ Atlantic Canada ◦ Alberta ◦ British Columbia (and the Yukon) ◦ Greater Toronto Area (GTA) ◦ Ontario (excluding GTA) ◦ The Prairies (SK,MB) and NT, NU	*Company Business Model* ◦ Sells directly to consumers ◦ Sells directly to other businesses/organizations ◦ Sells directly to both consumers and other businesses/organizations *Business size*: ◦ Self-employed (1 employee) ◦ 2-4 employees ◦ 5-9 ◦ 10-19 ◦ 20-99 ◦ 100 or more employees

[8] 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).

Annex 2: Tabulated Data

A full set of tabulated data (under separate cover)

Annex 3: Research Instrument

Hello, my name is [Interviewer's name]. 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 10 minutes. Please note that your responses will be kept entirely confidential and anonymous, and that this survey is registered with the Marketing Research and Intelligence Association (MRIA).

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 IS SHOULD TAKE APPROXIMATELY 10 MINUTES.

IF RESPONDENT QUESTIONS THE VALIDITY OF THE SURVEY, OFFER TO FAX/EMAIL HIM/HER THE VALIDATION LETTER FROM THE OPC. IF THIS DOES NOT SATISFY THE POTENTIAL RESPONDENT, ASK HIM/HER TO CALL HEATHER ORMEROD OF THE OFFICE OF THE PRIVACY COMMISSIONER AT 819-994-5682 (OR HAVE HEATHER CALL THE RESPONDENT).

IF RESPONDENT ASKS, THE SURVEY IS REGISTERD 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: T2013 = TRACKING (T) FROM THE 2013 BUSINESS SURVEY.

SECTION HEADINGS 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) T2013

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)

*INTERVIEWER NOTE: IF ASKED ABOUT RESPONSE OPTION (1) "CONSUMERS", SAY: This refers to an individual not a business or organization.

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

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. T2013

3. Which of the following types of personal information does your company collect about your customers? (READ LIST. ACCEPT ALL THAT APPLY) T2013-MODIFIED

Contact information, such as names, phone numbers, and addresses	1
Opinions, evaluations, and comments	2
Purchasing habits	3
Financial	4
Medical information	5
Driver's license numbers	6
Social Insurance Numbers	7
Other information. (DO NOT READ) If so, please specify: _____	9
None of the above (DO NOT READ)	10

4. In which of the following ways does your company store personal information on your customers? Is the information…? (READ LIST. ACCEPT ALL THAT APPLY) T2013

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. (DO NOT READ) 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.

5. What steps do you take to protect the personal information on your customers? Do you use…. (READ LIST. ACCEPT ALL THAT APPLY) T2013-MODIFIED

Physical measures, such as locked filing cabinets, restricting access, or security alarms.	1
Passwords	2
Encryption*	3
Firewalls	4
Organizational controls, such as policies and procedures.	5
Some other measure. (DO NOT READ) If so, please specify: _____	6
No measures taken	7

*INTERVIEWER NOTE. IF ASKED ABOUT ENCRYPTION, SAY: Encryption involves using an algorithm to transform information into text that is unreadable without a "key" to read the code.

6. Have you designated someone in your company to be responsible for privacy issues and personal information that your company holds? T2013

Yes	1
No	2

7. Has your business developed and documented internal policies for staff that address your privacy obligations under the law? T2013

Yes	1
No	2

8. Does your organization regularly provide staff with privacy training and education? T2013

Yes	1
No	2

9. Does your company have procedures in place for responding to customer requests for access to their personal information? T2013

Yes	1
No	2

10. Does your company have procedures in place for dealing with complaints from customers who feel that their information has been handled improperly? T2013

Yes	1
No	2

11. Does your company have a privacy policy that explains to customers how you will collect and use their personal information? T2013

Yes	1
No	2

SECTION 2: PRIVACY AS CORPORATE OBJECTIVE

12. 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. T2013

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. T2013

13. 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. T2013

14. 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. T2013

SECTION 4: COMPLIANCE

15. Still thinking specifically about PIPEDA, has your company taken steps to ensure that it complies with the federal government's privacy law?

Yes	1
No	2

IF YES:

16. Was it difficult for your company to comply with PIPEDA?

Yes	1
No	2

IF YES:

17. In your view, what was the most significant barrier or challenge for your company in terms of complying with PIPEDA? (READ LIST. ACCEPT MULTIPLE RESPONSES) T2013-MODIFIED

Not having a clear understanding of the legislation	1
The staff/personnel time needed to comply	2
The cost of compliance (excluding staff costs)	3
Enforcing compliance among employees	4
Other: (DO NOT READ) Specify _____	

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. T2013

18. 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. T2013

19. 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? T2013

Yes	1
No	2

SECTION 6: CORPORATE INNOVATION

20. 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. T2013

Yes	1
No	2

21. 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? T2013

Yes	1
No	2

22. Does your company allow employees to use personal electronic devices, such as smartphones, tablets, PCs, or other electronic devices, for work purposes, such as accessing company networks or data? ? [READ LIST. ACCEPT ONE RESPONSE]

Yes	1
No	2

SECTION 7: COMMUNICATIONS

23. What organizations or resources does your company use, if any, to help clarify its responsibilities under Canada's privacy laws?

Internet (general)	1
Government [PROBE WHETHER FEDERAL (2A) OR PROVINCIAL (2B)]	2*
Privacy Commissioner [PROBE WHETHER FEDERAL (3A) OR PROVINCIAL (3B)]	3*
Lawyer	4
Company/head office expert/internal resource for company	5
Industry experts, consulting firms, or education sources	6
Industry association	7
None/Do not use	8
Other. Specify: _____	

SECTION 8: OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

24. 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? T2013

Yes	1
No	2

SECTION 9: CORPORATE PROFILE

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

25. 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)

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

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

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

27. In which of the following categories would your company's 2014 revenues fall? (READ LIST. ACCEPT ONE RESPONSE)

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.

Annex 4: Statement of Political Neutrality

Political Neutrality Certification:

I hereby certify as a Senior Officer of Phoenix Strategic Perspectives that the deliverables fully comply with the Government of Canada political neutrality requirements outlined in the *Communications Policy* of the Government of Canada and Procedures for Planning and Contracting Public Opinion Research. Specifically, the deliverables do not contain any reference to electoral voting intentions, political party preferences, standings with the electorate, or ratings of the performance of a political party or its leader.

Original signed by

Alethea Woods
President
Phoenix Strategic Perspectives Inc.