Cross-National Study of Canadian and U.S. Corporate Privacy Practices

Presented by

Ponemon Institute

and the

Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner/Ontario

Ponemon Institute

Sponsored by

Carlson Marketing Group®

World Leader in Relationship Marketing

May 2004

Acknowledgements

This paper summarizes the findings of a benchmark study conducted by the Office of the Information and Privacy Commissioner of Ontario and Ponemon Institute – a Tucson, Arizona based "think tank" dedicated to the advancement of responsible information management practices within business and government. Carlson Marketing Group Canada serves as the exclusive sponsor of this empirical benchmark study.

Ponemon Institute extends its sincere appreciation to Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Brian Beamish and other members of the IPC executive staff, for providing guidance and support throughout this project. Without Ann's intellectual insight, intuition and assistance throughout the course of the study this work would not have been possible. We also extend our thanks to Professor Marilyn Greenstein, Arizona State University West, for helping us with the conceptual design of the cross-national research.

A special thank you is extended to members of Ponemon Institute's Responsible Information Management Council for providing support, guidance and expert counsel in the preparation of the survey instrument and validation of key research findings. We greatly appreciate the constructive feedback provided on earlier versions of this paper from Peter Cullen, Microsoft Corporation, Sandy Hughes, Procter & Gamble, Charles Giordano, Bell Canada, Shahriar Beigi, Unisys Corporation, Barbara Lawler, Hewlett Packard, and Trevor Hughes, International Association of Privacy Professionals.

Most importantly, we extend a special thank you to 38 Canadian and U.S. companies that participated in our joint study. Without their co-operation, transparency and constructive feedback, this paper would forever be in the planning stage.

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario CANADA
M4W 1A8
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Ponemon Institute
Attn: Research Department
3901 S. Escalante Ridge Place
Tucson, Arizona 85730
520-290-3400
research@ponemon.org

Table of Contents

I. Executive Summary

Ponemon Institute and the Office of the Information and Privacy Commissioner of Ontario (IPC) are pleased to present the summary results of the first study that benchmarks the corporate privacy practices of Canadian and U.S. companies. The Carlson Marketing Group Canada serves as the exclusive sponsor of this important study.

Results from the *Cross-National Study of Canadian and U.S. Corporate Privacy Practices* (hereafter termed the Study) provide a meaningful baseline for measuring and monitoring trends about how organizations in two neighboring but different countries are facing regulatory requirements and creating privacy programs that build trust with their key stakeholders.

Drawing from a representative sample of 19 Canadian companies and a matched sample of 19 U.S. companies, the Study addresses eight key areas in the typical corporate privacy program.[1] The eight areas are: Privacy Policy, Communications and Training, Privacy Management, Data Security Methods, Privacy Compliance, Choice and Consent, Global Standards and Redress.

A comprehensive privacy and data protection program with these eight areas is becoming increasingly important for several reasons. These include, but are not limited to:

- The organization's need to comply with the plethora of emerging privacy legislation and regulation;
- The adoption of enabling technologies in the collection, use and storage of personal data; and
- The increased expectation that organizations will take the necessary steps to safeguard their privacy commitments to customers, consumers and employees.

Findings of the Study suggest that most U.S. corporations are approaching their privacy initiative as one restricted to compliance and risk management. In this study, only 17% of privacy leaders in U.S. companies believe that corporate privacy is an important part of corporate brand or image in the marketplace. This does not appear to be true among Canadian companies. More than 61% of Canadian companies connect good privacy practices with enhanced customer trust and loyalty to the brand.

Canadian privacy leaders seem to understand and respect the need for compliance with federal and provincial laws and requirements. However, they rarely see compliance as the single goal or mission of privacy management. Canadian privacy leaders are more likely to hold the view or belief that their role is inextricably tied to information ethics rather than obedience to the law.

[1] Most of Canadian companies in this study are divisions or wholly owned affiliates of companies headquartered in the United States. Only seven companies are headquartered in Canada without affiliation with a U.S. parent.

Our study provides comparative information on what Canadian and U.S. companies are doing to achieve privacy programs that protect sensitive personal information about customers, target customers and employees. This study also seeks to determine what companies are doing to move beyond compliance with regulations. We want to understand if progressive companies are starting to view privacy as an opportunity to build trusted relationships with stakeholders to increase revenue and strengthen reputation and brand.

Key Findings

1. Canadian companies are more likely to have a dedicated privacy officer or leader responsible for privacy issues than comparable U.S. companies. In addition, privacy programs in Canadian firms tend to have a clearly articulated strategy, mission and charter. Canadian privacy leaders are more likely to have high level reporting authority and access to significant resources within their organization.

2. Canadian companies are more likely to have a formal redress process for customers and other stakeholders to respond to queries and concerns about how personal information is used, shared and retained. Similarly, Canadian companies are more open to providing customers with access rights to see and correct personal information collected about them and their families.

3. While Canadian and U.S. privacy policies have similar language and nearly identical levels of complexity, Canadian policies appear to offer more choice to customers and consumers in terms of opting out (or opting in) to secondary uses and sharing. In addition, while data sharing with third parties is a common practice in both Canada and the U.S., none of the Canadian companies actually permitted the sale of customer data.

4. Canadian companies are more likely to offer privacy training or awareness programs for employees and contractors who handle sensitive personal information than comparable U.S. companies.

5. Corporate marketers in Canadian companies appear to be more involved in their company's privacy initiatives than comparable U.S. companies.

6. Canadian companies appear to hold their vendors and other third parties to higher standards or due diligence requirements. This is especially the case for companies that acquire sensitive personal data for legitimate business purposes. There is no clear evidence, however, that Canadian companies are more aggressive at monitoring or enforcing these standards than comparable U.S. companies.

7. Canadian companies appear to have a more aggressive data control orientation when collecting and retaining sensitive personal information. Canadian companies are more concerned about insider misuse than external penetration.

8. Canadian companies appear to require more rigorous data quality controls and monitoring requirements for transacting and moving of personal information about employees and customers, especially when the application involves transborder movement.

9. U.S. companies use more rigorous data security mechanisms and controls to prevent potential hackers from penetrating the company's IT core and data warehouses.

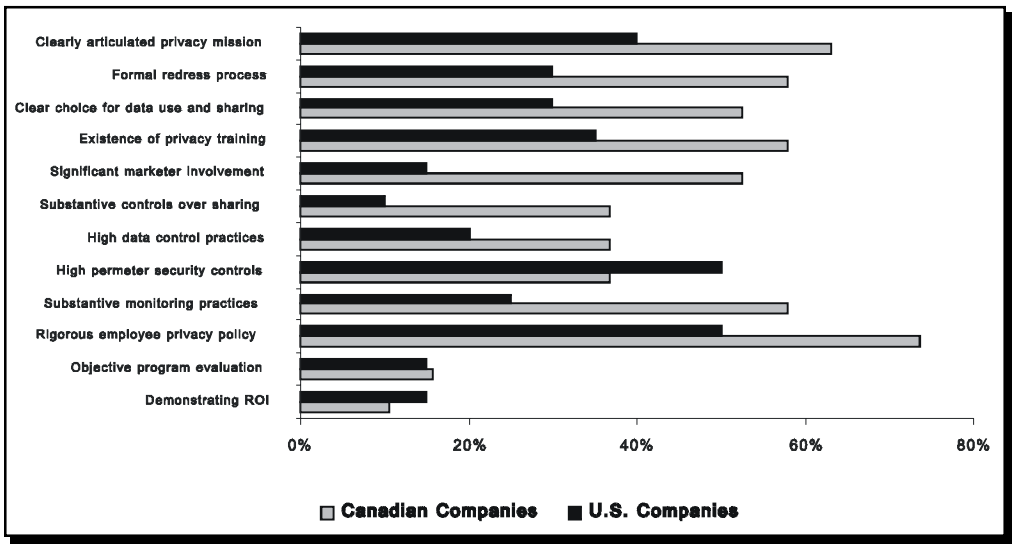
10. U.S. companies are less likely to have strict policies that protect the privacy of employees' personal data and records. In Canadian companies there are few policies governing the monitoring and surveillance of employee computer usage in the workplace.

11. Both Canadian and U.S. companies have a difficult time measuring the effectiveness of specific controls intended to reduce privacy risks.

12. Both Canadian and U.S. companies have an equally difficult time proving the economic value of privacy and data protection on corporate profitability (ROI).

Bar Chart 1 summarizes the 12 most salient differences between our representative samples of Canadian and U.S. companies. Please note that some of these characteristics were derived from combined survey results and followup interviews with participating Canadian and U.S. companies.

Bar Chart 1.



II. Introduction and Caveats

This report provides the results of a small, non-scientific benchmark study about the corporate privacy and data protection practices of business organizations in Canada and the U.S. Ponemon Institute is a "think tank" dedicated to the study of responsible information management practices within business and government. While we conducted this research in collaboration with the IPC, all empirical results were captured, compiled and analyzed independently by the Institute.

Privacy management is a relatively new organizational activity in many organizations. As a consequence, there is a lack of information about the practices and processes employed by companies to mitigate business risk and ensure compliance. This study seeks to shed light on the emerging area of privacy management by attempting to answer four basic questions:

1. What are leading companies doing today to ensure adequate compliance with the rash of new privacy and data protection compliance requirements in Canada and the U.S.?

2. Is there a common set of business practices employed by leading companies in Canada and the U.S. today to ensure reasonable protection and controls over the collection, use, sharing and protection of personal information?

3. Are there apparent gaps in privacy and data protection activities that create vulnerabilities for companies in terms of their privacy and data protection responsibilities?

4. Do Canadian and U.S. corporate privacy and data protection practices differ? If so, are these differences due to regulation or cultural orientation to responsible information management?

Because this is the first benchmark study that seeks to compare Canadian and U.S. companies, we anticipate that there will be many open issues and potential areas for future improvement to the basic research. We welcome your suggestions and constructive input before implementing follow-up studies.

Caveats on Benchmark Findings

There are inherent limitations to survey research that need to be carefully considered before drawing conclusions from findings. The following items are specific limitations that are germane to the present study.

- **Non-statistical results.** The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative (non-statistical) sample of large organizations, mostly composed of Canadian or U.S. publicly listed corporations. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature and sampling process used.

- **Sampling-frame bias.** The current findings are based on a small representative sample of completed surveys. As explained below, companies were preselected and contacted by Ponemon Institute or the IPC based solely on organizational size and reputation. Non-response bias was not tested, so it is always possible companies that did not participate are substantially different in terms of benchmark performance criteria from those that completed the instrument.

- **Company-specific information.** The benchmark information is sensitive and confidential. Thus, the collection instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.

- **Unmeasured factors.** To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.

- **Self-reported results.** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that self-reported results are inherently subjective and may tend to be biased.

III. Benchmark Survey Methods

The benchmark survey is designed to collect descriptive information from privacy and data protection practitioners in a timely and cost-efficient manner. The number of survey items is limited to key business issues that cut across different industry sectors. We believe that a survey focusing on business issues (rather than compliance issues) yields a higher response rate and better quality of results. We also use a paper instrument, rather than electronic (web) survey, to provide greater assurances of confidentiality.

To keep the survey to a manageable size, we carefully limited items to only those business factors that we consider crucial to the research objective. Hence, items focus on eight core areas of privacy management across the enterprise. Other descriptive items explore key relationships between organizational variables and descriptive responses to benchmark items.

Ponemon Institute developed a proprietary benchmark survey instrument in an earlier study presented as a keynote presentation at a Federal Trade Commission workshop held in June 2003.[2] The instrument used in the present study was modified to capture questions that focus on cross-national differences in privacy compliance. The edited version of the instrument was reviewed and approved by the IPC before launching data collection efforts.

In total, the benchmark survey instrument contains 108 descriptive items, all reported in Tables 1 to 8 of this report. The study captures organizational demographic items for sample analysis and comparison (as an appendix to the survey instrument). A fixed-format design is used for capturing responses to all benchmark items. The following are the fixed response categories to all benchmark items:

Yes	Denotes a positive response to one survey item.
No	Denotes a negative response to one survey item.
Unsure	Denotes sufficient information available to the individual responding to one survey item.
Exception	Which is additional contextual information to explain, Yes, No or Unsure responses to each given survey item. This data is optional only.
Blank	This is a no comment response and is not counted in the analysis.

Analysis of benchmark responses focuses on the percent of positive (Yes) responses, defined as:

Yes (Adjusted for Reverse Scored Items)/(No + Unsure)

[2] International Association of Privacy Professionals and Ponemon Institute *2003 Benchmark Study of Corporate Privacy Practices*: Working paper presented at United States Federal Trade Commission Workshop on Privacy, June 5, 2003.

The percent of Yes response variable is our surrogate for measuring good privacy practices. No, Unsure or Blank responses provide insufficient information to draw any conclusions about the efficacy of corporate privacy efforts.

A secondary variable reported in the analysis is the percent of completion. When all participating companies responded to the item with either a Yes, No or Unsure response (i.e., not Blank) it means that there is a 100% completion rate. Only four items achieved 100% response from all participating Canadian and U.S. companies. The average percent of completion to all 108 items is 86.5%, with the lowest rate at 46%. The item-by-item percent of completion rates are reported next to the percent of positive responses.

Assurances were provided by the Institute and IPC that company-specific information would not be revealed without the express consent or permission of the company. Ponemon Institute also signed strict one-way confidentiality agreements to ensure compliance to our own data privacy commitments.

The IPC and Ponemon Institute made personal contact to numerous organizations that were deemed to be good candidates for participation based on their size and reputation for good data management practices. Most of this outreach effort occurred in the late fall of 2003. Additional outreach efforts were made by the researchers in the early 2004 timeframe.

The survey instrument does not capture company-specific information of any kind. Subject materials contain no tracking codes or other methods that could link responses to identity. In some instances, subjects returned their survey in a business envelope. In these cases, we removed the instrument and destroyed the envelope. In other instances, individuals sent their completed survey through e-mail. Again, in these cases, the instrument was printed and the e-mail immediately deleted.

Each instrument was completed by the company and carefully screened by the researcher to determine completeness and assess accuracy. Only one instrument was rejected based on too many incomplete or blank responses. In addition, each instrument was reviewed for consistency. Another two instruments were rejected because of inconsistent or erroneous responses.

Our sampling procedure was organized into two stages. The first stage was to select large multinational companies with significant operations in both Canada and the U.S. This allowed us achieve a matching or side-by-side comparison of results. In total, 12 companies in this study provided separate benchmark surveys for both their Canadian and U.S. divisions. This results in 24 separate entities for analysis.

The second stage of our sample was to select organizations that had a Canadian presence with a U.S. affiliate or parent. Another seven Canadian-only organizations participated. These companies were matched to a U.S.-based company based on industry and approximate organization size.[3]

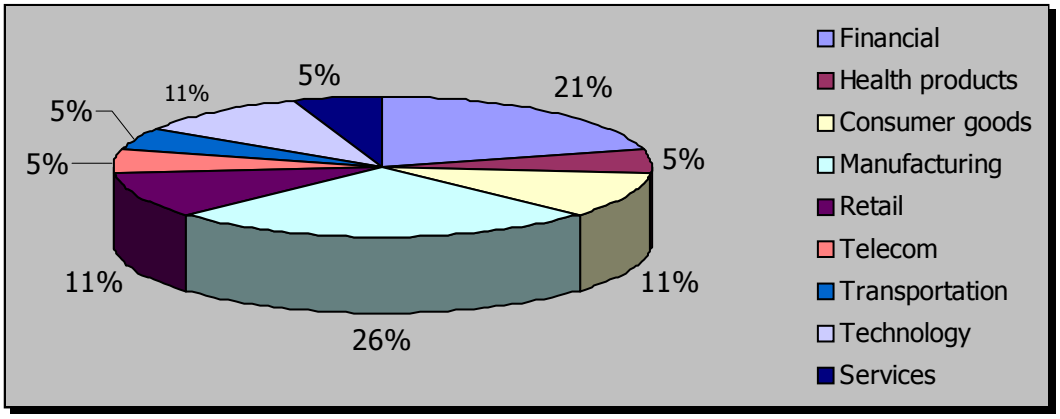
The following matrix provides a simple summary recap of sample response results from Canadian (19) and U.S. (19) companies, totaling 38 separate benchmark surveys.

Table 1: Sample Characteristics

	Frequency
Total number of companies contacted for participation	61
Total number of companies with both U.S. and Canadian companies participating in study	12
Total number of separate survey units to analyze	24
Total number of companies with only Canadian operations	7
Total number of industry matched companies in U.S.	7
Total number of companies in sample	38

Pie Chart 1 below shows the distribution of 38 companies analyzed in this report, according to their self-reported industry classification. The largest sample segments are manufacturing (26%) and financial services (21%). Retail, technology and consumer goods are each 11% of the total sample. The remaining industry groups, each representing only 5% of the sample, include: telecom, transportation, health products and services.

Pie Chart 1

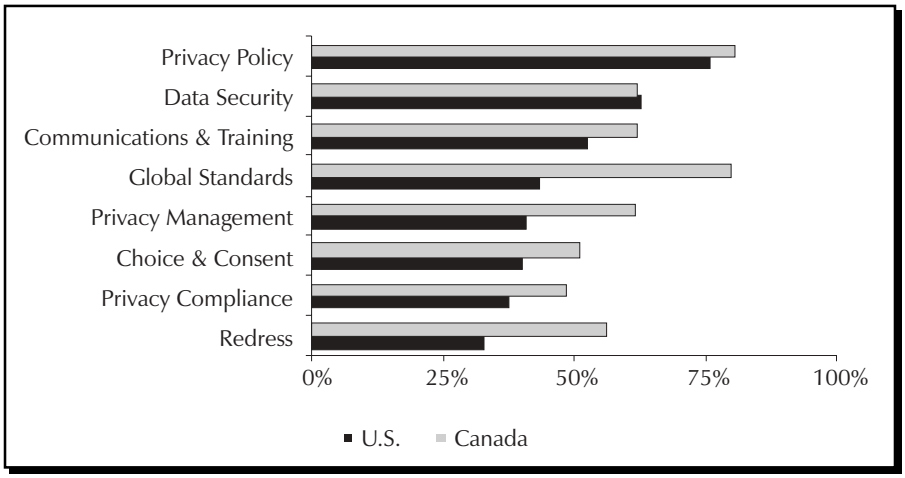


[3] Please note that all of the U.S. companies matched to the Canadian-only sub-sample were participants in the earlier benchmark study presented to the FTC workshop on June 5, 2003.

IV. Results of the Study

Our benchmark results are presented according to the eight broadly defined categories of privacy program management from the survey instrument. Bar Chart 2 reports summarized benchmark survey responses according to all eight categories examined for the Canadian and U.S. benchmark sub-samples.

Bar Chart 2: Percentage positive response to eight (8) privacy program categories for U.S. and Canadian



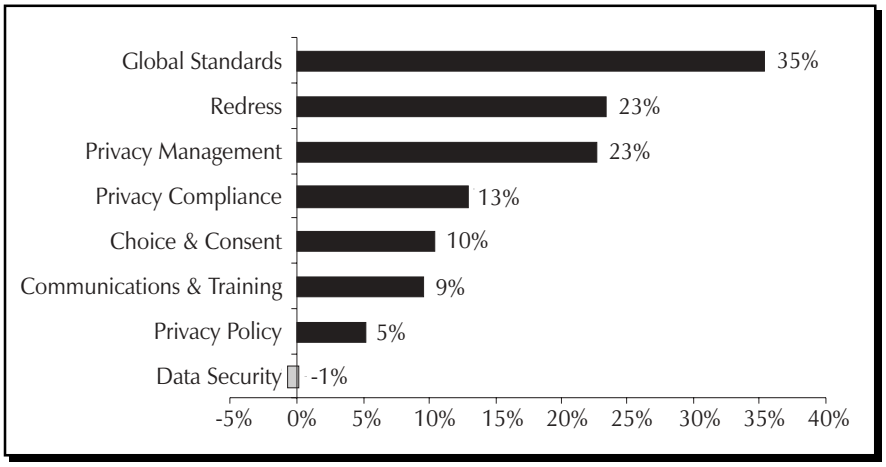
This chart shows where companies are devoting most of their efforts and resources. The percent of positive responses across eight categories varies considerably for both U.S. and Canadian companies. For U.S. companies, the most common privacy activities concern policy and data security. The least common activities concern redress. For Canadian companies, the most common activities concern policy and global standards. Redress activities appear to be more common for Canadian companies than U.S. firms.[4]

Bar Chart 3 provides benchmark survey differences between U.S. and Canadian companies. The variable **Diff** is defined as the overall benchmark category difference between Canadian and U.S. companies. A positive **Diff** implies that the Canadian results outperform U.S. results, and a negative **Diff** implies the opposite.

As can be seen, with the exception of the data security category (**Diff** = -1), Canadian companies outperform U.S. companies. The most significant benchmark survey differences pertain to the implementation of global standards (**Diff** = 35%), redress (**Diff** = 23%), and privacy management (**Diff** = 23%). These results provide evidence that Canadian companies achieve more success in launching key privacy program initiatives in comparison to the matched sample of U.S. firms.

[4] Please note that these results track closely to earlier benchmark survey results reported in the IAPP & Ponemon Institute *2003 Benchmark Study of Corporate Privacy Practices*.

Bar Chart 3: Percentage difference (Diff) between Canadian and U.S. companies according to eight (8) privacy program categories



Benchmark on Corporate Privacy Policy

The primary purpose of a privacy policy is to document the company's practices and procedures for collecting, using, sharing and protecting personal information about customers, consumers and employees. Table 2 reports the summarized results for benchmark survey items pertaining to corporate privacy policies for U.S. and Canadian companies.

Table 2: Summary of Benchmark Survey Responses for Match Sample of U.S. (n_1=19) and Canadian (n_2=19) Companies

	U.S.	Canada	PCT%
Privacy Policy	Pct% Yes	Pct% Yes	Diff
Does your company have a privacy policy?	100%	100%	0%
Does your company have a separate privacy policy for employees?	83%	89%	6%
Does your company align its privacy policy with the expectations of stakeholders?	56%	73%	17%
Does your company align the privacy policy with its business conduct or ethics policy?	95%	100%	5%
Does the privacy policy address industry trends and issues?	72%	78%	6%
Is there more than one privacy policy within your organization?	44%	41%	-3%
If multiple policies exist, is there a process in place to ensure the policies are consistent?	67%	75%	8%

	U.S.	Canada	PCT%
Privacy Policy	Pct% Yes	Pct% Yes	Diff
Does your company have a "version control" process over privacy policies and notices?	72%	78%	6%
Do you coordinate privacy policies between U.S. and Canadian subsidiaries or divisions?	76%	78%	1%
Does your company have formal controls over revising the privacy policy?	94%	100%	6%
Is the privacy policy reviewed and approved by the CEO or other senior executive?	72%	74%	1%

As shown, all participating companies (100%) have a privacy policy and over 70% have the policy reviewed and approved by a senior executive before it is published. Many companies have separate privacy policies for consumers and employees, and most companies attempt to align their policies with a code of business conduct or ethics. Less than half of U.S. and Canadian companies have separate policies for their business segments, divisions, units or functions. While there are differences between U.S. and Canadian companies in this category, these differences are especially significant in one area – namely, the degree to which the companies align their policy with expectation of stakeholders. Accordingly, Canadian companies appear to spend more effort vetting policies before key stakeholder groups than U.S. firms.

Benchmark on Privacy Communication and Training

Table 3 reports the summarized results for benchmark survey items pertaining to corporate communications, training and awareness activities.

As noted below, an overwhelming majority of respondents have privacy policies for their companies. However, 40% of U.S. companies and 54% of Canadian firms report that these policies may be written using language that is too difficult for the average person to read and comprehend.

Moreover, it is not certain whether customers have a reasonable understanding of the company's privacy policy. While 94% of respondents report that they have a process in place to disseminate privacy policy information to consumers and their customers, only 50% of U.S. companies have an ongoing privacy training program. In sharp contrast, 82% of Canadian companies have formal programs to create awareness or educate employees about privacy. The most typical method for reaching customers for both U.S. and Canadian firms (89%) is to post the policy on the company's website.

In the area of communication and training, survey results suggest that Canadian companies are doing a reasonable job in creating awareness and understanding of privacy procedures among new employees (71%), but this may not be the case for U.S. firms (43%). It is unclear whether employees in Canadian and U.S. companies are given the appropriate training and support in order to be able to apply privacy procedures to mitigate information risks resulting from given job functions. Specifically, only 53% of Canadian companies and 40% of U.S. companies have mandatory training for employees who handle sensitive personal information.

Table 3: Summary of Benchmark Survey Responses for Match Sample of U.S. (n_1=19) and Canadian (n_2=19) Companies

	U.S.	Canada	PCT%
Communication and Training	Pct% Yes	Pct% Yes	Diff
Is there a process for communicating the privacy policy to all employees?	94%	94%	0%
Is the privacy policy posted on the company's website?	89%	89%	0%
Is there a process for communicating the privacy policy to all customers and consumers?	80%	83%	3%
Does your company share the privacy policy or notice with its business partners?	69%	72%	3%
Do business partners have the ability to learn more about the company's privacy policy?	69%	72%	3%
Does your company have an ongoing privacy training program in place?	50%	82%	32%
Does your company have a privacy awareness activity for new employees?	43%	71%	28%
Is there a process for distributing privacy notices to customers and consumers?	58%	69%	10%
Does your company have formal controls over communicating policy change?	50%	64%	14%
Is privacy training mandatory for employees who handle sensitive personal information?	40%	53%	13%
Is the privacy policy easy to understand (written at an eighth-grade level of reading)?	40%	54%	14%
Are e-learning modules available to employees for on-demand training?	50%	44%	-6%

	U.S.	Canada	PCT%
Communication and Training	Pct% Yes	Pct% Yes	Diff
Are the results of privacy training communicated to senior executives or the Board?	27%	25%	-2%
Is the privacy training program customized by job function or business risk?	54%	65%	11%
Is there a privacy awareness effort or outreach to new customers?	45%	57%	12%
Are performance measures in place to determine the effectiveness of privacy training?	23%	38%	14%
Is privacy training available to business partners?	0%	6%	6%

Furthermore, only 27% of U.S. companies and 25% of Canadian companies communicate the results of privacy education and training to senior management or the board of directors. In addition, only 23% of U.S. companies and 38% of Canadian firms attempt to measure the effectiveness of their training programs.

While about 70% of companies share their privacy policy with business partners (such as vendors, contractors, joint venture partners and so forth), no U.S. companies – and only one Canadian firm – offer their privacy awareness and training initiatives to business partners.

Benchmark on Privacy Management

The role of the privacy professional in many organizations is a relatively new one. As a result, there is a dearth of information about the nature and structure of the privacy function within corporations. Based on the findings, however, it appears that as a business management issue, privacy is not high on the radar screen of executives.

Table 4 summarizes the benchmark results for privacy management activities. The findings from this section of the survey offer revealing insights about how respondents view privacy as a business issue within their organizations.

One of the most salient findings is that 36% of U.S. respondents believe that their resources are inadequate to achieve their companies' privacy compliance objectives. In contrast, over 71% of Canadian firms believe they have adequate resources.

Another major finding concerns respondent's belief about the importance of privacy to their company's brand or marketplace image. Only 17% of U.S. companies believe that privacy is important to their firm's corporate image or brand, while over 60% of Canadian companies believe this to be the case.

Table 4: Summary of Benchmark Survey Responses for Match Sample of U.S. (n_1=19) and Canadian (n_2=19) Companies

	U.S.	Canada	PCT%
Privacy Management	Pct% Yes	Pct% Yes	Diff
Does your company require business partners to comply with its privacy policy?	31%	73%	42%
Do standard business contracts contain language to ensure privacy protections?	81%	94%	13%
Is there a cross-functional committee involved in managing the privacy initiative?	89%	94%	5%
Does the committee have formal responsibilities and a charter?	40%	81%	41%
Does your company have a senior executive (CPO) responsible for privacy?	50%	76%	26%
Is the company's chief privacy officer the chairman of the committee?	33%	67%	33%
Are business partners monitored or vetted for compliance with the privacy policy?	36%	30%	-6%
Does the privacy program have sufficient resources to achieve its objectives?	36%	71%	35%
Does your company comply with a major privacy seal or certification?	50%	38%	-12%
Does the privacy officer report directly to senior management (such as the CEO)?	19%	54%	35%
Is privacy an important part of the company's brand or marketplace image?	17%	61%	44%
Is there a formal process for measuring managers' compliance with the privacy policy?	23%	29%	5%
Is the privacy leader fully dedicated to the privacy program (a full-time job)?	33%	65%	31%
Has an independent privacy audit been conducted within the last two years?	27%	27%	0%

About 90% percent of companies have a cross-functional committee to manage their privacy initiatives. However, only 40% of U.S. firms have a formal charter or mission that is defined for the committee. In sharp contrast, over 81 of Canadian firms have a formal charter or mission statement for defining the committee's governance responsibilities.

Over 50% of U.S. companies and 76% of Canadian companies have designated one individual to lead the company's privacy initiative. Only 19% of U.S. privacy leaders (Chief Privacy Officers or CPOs) report directly to senior leadership such as the division president or CEO. However, over 54% of Canadian companies have privacy leaders who report to senior executives.

Without full-time privacy officers reporting directly to the most senior level of management and with insufficient resources to ensure that privacy goals are met, it appears that privacy might not be as high a priority as other issues faced by U.S. companies. This may not be the case for Canadian companies, however.

To demonstrate their commitment to privacy and data protection, about half of U.S. companies and 38% of Canadian firms seek to comply with major privacy seal programs. However, less than 30% of companies attempt to measure how key managers comply with privacy regulations. Only 27% of both U.S. and Canadian companies have had an independent privacy audit in the last two years.

Most U.S. and Canadian companies (81% and 94%, respectively) require their business partners to comply with their privacy policies, and they have standard language in their contracts to that effect. However, approximately 36% of U.S. companies and 30% of Canadian firms do not perform monitoring of their business partners' compliance to standard contract terms.

Benchmark on Data Security

One objective of the study was to determine the processes involved to secure access and unauthorized use of personal information, and the enabling technologies companies use to protect sensitive information.

The benchmark results for both U.S. and Canadian companies to numerous data security items are summarized in Table 5.

Table 5: Summary of Benchmark Survey Responses for Match Sample of U.S. (n_1=19) and Canadian (n_2=19) Companies

	U.S.	Canada	PCT%
Privacy Security Methods	Pct% Yes	Pct% Yes	Diff
Does the company capture SSN or SIN numbers of employees for ID mgmt?	83%	82%	-1%
Does your company take an inventory of the personal information collected and used?	63%	65%	2%
Does your company have a privacy and data protection strategy?	64%	64%	0%

	U.S.	Canada	PCT%
Privacy Security Methods	Pct% Yes	Pct% Yes	Diff
Are new software applications and databases reviewed for privacy before production?	64%	62%	-2%
Are privacy-enabling technologies used within the company?	19%	21%	3%
Does each web page that captures personal information link to posted policy?	50%	65%	15%
Does the company capture SSN or SIN of customers for identification and authentication?	63%	56%	-6%
Does your company review website content for privacy compliance before publication?	65%	56%	-8%
Are third-party cookies used on your company's website?	58%	59%	1%
Does your company capture privacy preferences of consumers and customers?	53%	79%	25%
Does your company have control over all domains linked to the primary web domain?	65%	36%	-29%
Does your company's website deploy the Platform for Privacy Preferences (P3P)?	17%	18%	1%
Are web beacons limited for use on company's websites?	65%	47%	-18%
Are data integration services used to improve the quality of customer information?	47%	53%	6%
Does your company systematically evaluate if individual permissions are being honored?	38%	65%	26%
Is information security integrated with privacy compliance?	47%	50%	3%
Does your company use SSL?	94%	92%	-2%
Does your company authenticate visitors to your website?	86%	85%	-1%
Does your company use authentication to determine access rights?	67%	76%	10%
Does your company use encryption in the exchange of customer information?	69%	67%	-2%
Does your company use encryption in the exchange of employee information?	56%	67%	10%
Does your company have firewalls over consumer data?	100%	79%	-21%
Does your company have firewalls over employee data?	88%	73%	-15%
Does your company use Intrusion detection systems (IDS) used over systems using or storing sensitive personal information?	81%	68%	-13%

Currently, approximately 50% of Canadian respondents and less than 47% of U.S. firms do not integrate information security with privacy initiatives. While over 65% of U.S. firms have complete control over all corporate website domains, only 36% of Canadian firms say this is true for them.

Many U.S. and Canadian companies capture the SSN or SIN numbers of employees (83% and 82%, respectively) and customers (50% and 65%, respectively) for identification and authentication purposes. However, all companies acknowledged the importance of providing highly secure access and limiting unauthorized use of individual identity information.

In the case of consumer data, 53% of U.S. and 79% of Canadian firms capture the privacy preferences of consumers or customers, and 38% of U.S. and 65% of Canadian firms take active steps to evaluate if choices (opt-in or opt-out) are being honoured.

Very few U.S. and Canadian companies are using privacy-enabling technologies (19% and 21%, respectively), or deploy the Platform for Privacy Preferences (17% and 18%, respectively). This low usage suggests either the allocation of resources for other technologies or a lack of understanding of how these technologies could contribute to the goals of the privacy program. However, most respondents use security perimeter controls to protect personal, sensitive information. These include firewalls over consumer and employee data. Intrusion detection systems over sensitive personal information are used by 81% of U.S. companies and 68% of Canadian firms. Over 94% of U.S. firms and 92% of Canadian companies use SSL for encrypting web-based transactions (including the movement of web to backend applications).

On a positive note, over 63% of U.S. firms and 65% of Canadian companies are conducting inventories of the personal data collected and retained by them. Approximately 64% of both U.S. and Canadian companies are developing an overall strategic plan for privacy and data protection. Many U.S. and Canadian companies (64% and 62%, respectively) state that they are developing preventive procedures to evaluate new software applications for privacy glitches before placing them into production systems.

Benchmark on Privacy Compliance

Self-reported results suggest that very few responding U.S. and Canadian companies have experienced a regulatory inquiry concerning privacy in the last three years, or experienced a significant privacy violation in the last three years. Despite low regulatory actions, more than 81% of U.S. respondents and 88% of Canadian firms report that privacy compliance is a significant regulatory concern, and most U.S. and all Canadian firms (81% and 100%, respectively) devote time and resources to monitoring emerging regulations.

More than 69% of U.S. companies and 88% of Canadian respondents believe their company's senior leadership supports privacy initiatives in the organization, but only 25% of U.S. and 44% of Canadian firms report to the company's board of directors on a regular basis (at least once per year). Table 6 summarizes the benchmark results for privacy compliance items.

Table 6: Summary of Benchmark Survey Responses for Match Sample of U.S. (n_1=19) and Canadian (n_2=19) Companies

	U.S.	Canada	PCT%
Privacy Compliance	Pct% Yes	Pct% Yes	Diff
Is senior management supportive of the privacy compliance program?	69%	88%	19%
Is privacy compliance a significant regulatory concern for the company?	81%	88%	7%
Does your company monitor emerging state or provincial privacy regulations?	83%	100%	17%
Does your company ensure that marketing campaigns are privacy compliant?	56%	71%	14%
Is the privacy monitoring conducted by internal auditors other auditing professionals?	40%	25%	-15%
Is privacy monitoring done on an ongoing basis?	42%	36%	-5%
Does your company monitor internal compliance with its privacy policy?	38%	53%	14%
Does the privacy leader report the results of privacy compliance to the Board?	25%	44%	19%
Does your company have a formal crisis management process for privacy violations?	44%	50%	6%
Does the privacy program include workplace surveillance and computer monitoring?	13%	69%	57%
Are mock regulatory assessments conducted to determine compliance risk areas?	23%	29%	5%
Does your company promote its privacy compliance efforts to its customers?	38%	53%	15%
Has the company undergone a privacy regulatory inquiry within the last 3 years?	14%	25%	11%
Has the company experienced a privacy violation that has been revealed in the media?	6%	13%	7%
Does your company self-report privacy violations to regulatory authorities?	25%	25%	0%
Has the company experienced a significant privacy violation within the last 3 years?	0%	6%	6%

Shaded items are reversed scored in computation of percent positive response rate.

While respondents may worry, are they prepared to deal with a privacy blowup? More than 44% of U.S. companies and 50% of Canadian firms have a crisis management plan or process. About 56% of U.S. firms and 71% of Canadian companies attempt to ensure that marketing campaigns are privacy compliant. Only 40% of U.S. firms and 25% of Canadian companies use internal auditing to monitor privacy compliance activities. Less than 42% of U.S. respondents and 36% of Canadian firms perform privacy monitoring on an ongoing basis. Very few U.S. and Canadian companies (23% and 29%, respectively) conduct mock regulatory assessments or audits.

Benchmark on Choice and Consent

Table 7 reports benchmark results for survey items pertaining to individual customer, consumer or employee choice and consent.

Table 7: Summary of Benchmark Survey Responses for Match Sample of U.S. (n_1=19) and Canadian (n_2=19) Companies

	U.S.	Canada	PCT%
Choice & Consent	Pct% Yes	Pct% Yes	Diff
Does your company share customer information with affiliated organizations?	76%	76%	0%
Does your company share customer information with nonaffiliated third-parties?	76%	47%	-29%
Does your company share employee data with affiliates?	56%	32%	-24%
Does your company share employee data with nonaffiliated third-parties?	39%	39%	0%
Are employees given a choice over the way personal information is collected?	47%	22%	-25%
Are employees given a choice over the way personal information is used?	44%	72%	28%
Does your company provide "opt-out" over the secondary use and sharing?	53%	79%	26%
Does your company provide "opt-in" over the secondary use and sharing?	17%	29%	13%
Is there flexibility in the way consumers and customers can communicate their choice?	38%	50%	12%

Shaded items were removed from computation of positive response rate because a Yes or No response to these questions can have ambiguous meaning.

This section of the survey seeks to determine how companies are managing the privacy preferences of their consumers, customers and employees. The majority of U.S. and Canadian companies are sharing customer-centric information with affiliates (76%). However, more U.S. companies (76%) report that they are sharing customer-centric records with third parties than their Canadian counterparts (47%). Approximately 53% of U.S. companies and 79% of Canadian firms provide opt-out choices of secondary use or sharing of their personal information. Only 38% of U.S. companies and 50% of Canadian firms acknowledge that their customers have flexibility (multiple methods or channels) to express their privacy preference.

More than 47% of U.S. companies and 22% of Canadian firms provide employees with choice over the way their personal information is collected. Approximately 44% of U.S. firms and 72% of Canadian companies provide choice over the ways employee's personal information is used (including sharing among affiliates and third parties).

Benchmark on Global Standards

If a business receives and processes personally identifiable data about individuals living in the European Union (E.U.), it is subject to data transfer restrictions by the national privacy laws of the E.U. countries from where the data is exported. Unfortunately, survey results suggest that many U.S. companies do not make global privacy compliance a priority. This does not appear to be the case among Canadian organizations. Table 8 reports the results of survey items regarding compliance with global standards.

According to survey results, 44% of U.S. companies and 63% of Canadian firms evaluate transborder data flows. The Safe Harbor Agreement offers advantages for U.S. companies, but also additional burdens for companies with overseas operations. It is, therefore, not surprising that only 33% percent of U.S. companies surveyed have signed on to the Safe Harbor Agreement. In sharp contrast, over 79% of Canadian firms state that they are in substantial compliance with E.U. data protection laws.

Table 8: Summary of Benchmark Survey Responses for Match Sample of U.S. (n_1=19) and Canadian (n_2=19) Companies

	U.S.	Canada	PCT%
Global Standards	Pct% Yes	Pct% Yes	Diff
Does your company evaluate compliance with global regulations and standards?	57%	79%	21%
Does you company attempt to comply with global privacy and data protection laws?	59%	79%	20%
Are national privacy practices, laws and regulations monitored by your company?	44%	88%	44%
Are your privacy policies written in multiple languages when appropriate?	44%	83%	40%
Are trans-border data flows evaluated for compliance with national privacy laws?	44%	63%	19%
Does your company attempt to comply with Canadian privacy regulations (PIPEDA)?	21%	89%	68%
Does your company attempt to comply with EU Data Protection Laws (or Safe Harbor)?	33%	79%	45%

A majority of U.S. companies (79%) are not taking firm steps to comply with new national Canadian regulations. Only 44% of U.S. companies translate privacy policies into native languages of customers and employee. About 83% of Canadian firms state that they take steps to translate policies. Approximately, 57% of U.S. firms and 79% of Canadian companies evaluate compliance with global regulations and standards.

Benchmark on Redress

The purpose of a privacy redress program is to have established procedures that enable companies to quickly respond to a privacy complaint. Such a program can help organizations reduce the likelihood of a public privacy crisis, and if necessary, quickly address any problems in their privacy policies and practices.

The responses to benchmark items pertaining to redress and the enforcement of privacy breaches are reported in Table 9.

Table 9: Summary of Benchmark Survey Responses for Match Sample of U.S. (n_1=19) and Canadian (n_2=19) Companies

	U.S.	Canada	PCT%
Redress	Pct% Yes	Pct% Yes	Diff
Can customers and consumers access and correct their personal information?	25%	71%	46%
Do customers and consumers have redress for resolving privacy concerns?	40%	63%	23%
Can employees access and correct their personal information?	94%	100%	6%
Do employees have access to a redress mechanism for resolving privacy concerns?	56%	82%	27%
Is the redress process clearly described in the privacy notice or policy?	31%	61%	30%
Do you have a help line to respond to privacy questions or report a problem?	15%	42%	26%
Does the company provide a standardized process for responding to help line calls?	0%	14%	14%
Does the company employ an outside ombudsman to resolve privacy complaints?	0%	12%	12%
Does the company have a specific timeline for investigating alleged privacy complaints?	57%	69%	12%
Does the company have a formal process for enforcing privacy violations?	19%	61%	42%
Does the redress process have specific reporting requirements to management?	21%	38%	17%

While 19% of U.S. companies have a process for determining how to enforce privacy violations, over 61% of Canadian firms report that they do have formal redress process in place. Only 21% of U.S. and 38% of Canadian companies regularly report privacy complaints to management. Also, no U.S. companies and very few Canadian firms employ an outside ombudsman to resolve privacy complaints or use help lines to capture customer complaints.

Over 57% of U.S. companies and 69% of Canadian firms have a specific timeline for investigating alleged privacy complaints. Most U.S. companies (94%) and all Canadian firms provide access to employees to read and correct personal information. About 56% of U.S. and 82% of Canadian companies provide employees with access to a redress mechanism for resolving concerns over how their personal information has been collected and used.

Only 25% of U.S. respondents provide consumers and customers with the ability to access and correct their personal information. In sharp contrast, 71% of Canadian companies state that they provide customers with access, including methods for correcting erroneous personal data about themselves and their families.

Approximately 31% of U.S. companies and 61% of Canadian firms describe the company's redress process in the privacy notice or publicly disclosed policy to customers and employees.

Conclusion

Despite a small benchmark sample, our cross-national comparison of corporate privacy practices suggests that Canadian companies outperform their U.S. counterparts in a number of important areas. It is also clear that both Canadian and U.S. companies have room for substantial improvements in the design and execution of their privacy initiatives.

Findings of this study show that leading companies are more likely to execute the following business practices as an integral part of their enterprise privacy program:[5]

- Integrate information security and privacy into one virtual team
- Incorporate perspectives of legal, marketing, human resources and IT into privacy strategy
- Centralize privacy program responsibility under one senior executive sponsor
- Whenever feasible, consider using privacy enabling technologies
- Empower local managers to get involved, especially in communications, training and outreach
- Obtain real budget authority to implement enterprise programs
- Build process standards that resemble six sigma or ISO programs
- Establish upstream communication and fair redress
- Conduct privacy impact assessments to objectively determine issues, problems and mistakes
- Provide good reporting and disclosure tools to all stakeholders
- Make sure you listen to customers about their privacy preferences, concerns and issues
- Balance privacy goals against **practical** business objectives
- Obtain trust seal to signal good privacy practices, especially in web and e-mail outreach to customers

According to our study, areas of greatest weakness and vulnerability include the objective measurement of program effectiveness and the monitoring of sensitive personal data collected about customers, target customers and employees. As the outsourcing of data management

[5] These leading business practices were also revealed in an earlier study of 55 multinational corporations. See the IAPP & Ponemon Institute *2003 Benchmark Study of Corporate Privacy Practices*.

functions to third parties (within and outside North America) becomes the prevalent business practice in Canada and the U.S, there will be an increased need for greater data privacy controls, due diligence and verification.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or e-mail:

Ponemon Institute
Attn: Research Department
3901 S. Escalante Ridge Place
Tucson, Arizona 85730
520-290-3400
research@ponemon.org

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario CANADA
M4W 1A8
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Ponemon Institute
Attn: Research Department
3901 S. Escalante Ridge Place
Tucson, Arizona 85730
520-290-3400
research@ponemon.org