Comparative Privacy Practice – Canada and the United States

Jeffrey H. McCully
Barrister & Solicitor
July 5, 2004

A groundbreaking study comparing the motivations, practices and procedures of Canadian and American business organizations, released in May, has concluded that there are major differences between the two countries. Based upon in-depth interviews with thirty-six large companies, held in late 2003 and early 2004, across various industries, the Ponemon Institute, an American think-tank, concluded that U.S. corporations base their privacy policies on risk management and compliance. However, Canadian companies associate their privacy policies with enhanced customer trust and brand loyalty. In other words, Canadians see privacy law compliance as productive overall business practice and business ethics, not just a mandatory compliance issue.

The research conducted by the Ponemon Institute was done in collaboration with the Ontario Information and Privacy Commissioner (IPC). The study examined 19 Canadian companies and 19 American companies. Most of the Canadian companies were divisions or wholly owned subsidiaries of U.S. companies. Only seven (7) of the Canadian companies were headquartered in Canada without affiliation with a U.S. parent.

This paper is a review of the results of the Ponemon Institute-IPC Study. It should not be relied upon as legal advice.

Privacy Program Categories

The study reviewed eight (8) key aspects of a corporate privacy program, namely, Privacy Policy, Privacy Management, Communications and Training, Data Security, Privacy Compliance, Choice and Consent, Global Standards and Redress. Each of these categories will be reviewed.

Caveats and Limitations of the Study

The study does begin by listing certain *caveats* about the results. First and foremost, it is important to note that the results are descriptive, rather than statistical. In the words of the study, "[t]he current study draws upon a representative (non-statistical) sample of large organizations, mostly composed of Canadian or U.S. publicly listed corporations". Additionally, "[s]tatistical inferences, margins or error and confidence intervals cannot be applied to these data given the nature and sampling process used". Other noted shortcomings of the study include the fact that findings are based on a small sample of completed surveys. Moreover, the quality of the research is based upon the integrity of responses received. So, self-reporting results, by the very nature, are subjective, and may tend to be biased. Overall, the authors wish to point out that this was a benchmark type survey, designed to collect descriptive information.

Business Sectors Responding

The sample was 38 companies, with the largest segments being manufacturing (26%) and financial services (21%). Retail, technology and consumer goods companies represented 11% of the sample each. The telecommunications, transportation, health products and services sectors represented 5% each. For those wanting to review and compare Privacy Policies, companies across sectors post their Policies on their websites.

Corporate Privacy Program Goals

The motivations for corporate privacy and data protection programs are many. Three of the most important ones are the following:

(a) growing legislative schemes and regulations, both nationally and cross-nationally;
(b) technology enabling the collection, use, storage and disclosure of personal information; and
(c) the increasing expectations on the part of clients, customers, consumers and employees.

Key Questions

The study attempted to answer four basic questions concerning privacy policies and practices:

1. What are companies doing to ensure adequate compliance with the rash of new privacy and data protection compliance requirements in Canada and the United States?
2. Is there a common set of business practices used by leading companies today to ensure reasonable protection over the collection, use and sharing of personal information?
3. Are there gaps in privacy and data protection activities that create vulnerabilities for companies?
4. Do Canadian and U.S. corporate privacy and data protection practices differ? If so, are differences due to regulation or cultural orientation to responsible information management?

The Key Findings

1. Canadian firms are far more likely to have a clearly articulated privacy strategy, mission and charter (35%), in line with global standards.

2. Canadian firms are far more likely to have a dedicated privacy officer, who is more likely to have a high level reporting authority and access to significant resources within the organization (23%).

3. Canadian firms are far more likely to have a formal redress process for customers and clients to respond to concerns about how their information is used, shared and stored, including the opportunity to see and to correct errors (23%).

4. Canadian companies are more likely to have formal training programs for employees or contractors who handle personal information (9%).

5. Canadian privacy policies offer more choice to clients in terms of opting out (in) to secondary uses for the information collected and sharing of it.

6. Corporate marketers in Canadian companies are more involved in their company's marketing initiatives.

7. Canadian companies have a more aggressive data control orientation when collecting and storing sensitive information. Canadian companies are more concerned with *insider misuse*, while U.S. companies are more concerned with *external penetration.*

8. American companies are more concerned about hackers penetrating their companies' IT core and data warehouses (1% more – Data security being the only one of the eight privacy program categories in which the U.S. exceeds the Canadian companies).

9. Canadian companies require more rigorous data quality control for moving information about employees and clients, especially across borders.

10. Canadians are less likely to monitor employee computer usage.

11. American companies are less likely to have policies protecting employee privacy.

12. Both American and Canadian companies have a *difficult time measuring the effectiveness of controls* intended to reduce privacy risks.

13. Both American and Canadian companies have a *difficult time proving the economic value* of privacy and data protection on corporate profitability (defined as Return on Investment).

Benchmark One: The Corporate Privacy Policy

The primary purpose of having a privacy policy is to document the organization's practices and procedures for collecting, using, storing and disposing of information about its constituents (clients, customers, consumers, employees). The major difference between the countries is that Canadian firms tend to spend more effort aligning its privacy policy with the expectations of its stakeholders.

Benchmark Two: Communications and Training

It is unclear if either Canada or the United States has sufficiently educated employees about privacy principles, so as to mitigate privacy-related risks. Certainly, while Canada is more likely to have privacy training for new and existing employees, only 53% of respondents in Canada make it mandatory, compared to 40% in the U.S. No U.S. companies and only one Canadian company offer privacy and awareness and training to business partners. In Canada, this is a potential problem as liability is shared. Also, most interesting is the fact that neither country effectively measures the effectiveness of training.

Benchmark Three: Privacy Management

Again, in this category, it is evident that Canadian companies are more concerned with privacy. More Canadian companies (76%) than American ones (50%) have a senior executive responsible for privacy. This senior officer is more likely to report to the senior management of the company, such as a Chief Executive Officer (54% to 19%). Also, Canadian companies are more likely to have sufficient resources to achieve objectives (71% to 36%). Additionally, and most interesting, is the fact that only 17% of American companies believe that privacy is important to their firm's image or brand, compared to 61% of Canadian companies.

Finally, though, neither country's companies have had sufficient privacy auditing performed in the past two years (27% each). This response tends to lead one to believe that concern for having adequate privacy safeguards in place has not reached the highest levels of consciousness in corporate management, yet. This may be due, in part, to the fact that laws are quite new. Or, it might be due to the fact that management does not believe in the importance of privacy, or in the seriousness of the sanctions that may await the board of directors that does not properly implement controls.

Benchmark Four: Data Security

Data security paints another picture; one in which the United States corporate sector is more advanced. American companies are 29% more likely to have control over all domains linked to the primary Web domain. American companies are more likely to have firewalls over both consumer (21%) and employee (15%) data. American companies are 13% more likely to use intrusion detection systems (IDS) over systems using or storing sensitive personal information.

Positively for both countries, 63% of American and 65% of Canadian companies are conducting inventories of personal data collected and retained by them. About 64% of both countries' companies develop an overall strategic plan to privacy and data protection.

Benchmark Five: Privacy Compliance

Despite the fact that regulatory inquiries are few to date, most companies are becoming more aware of the changes to the regulatory landscape. Over 80%of firms report that privacy compliance is a regulatory concern. Most U.S. (81%) and all Canadian (100%) companies surveyed devote time and resources to monitoring emerging requirements.

Interestingly, however, much lower numbers are reported in both countries when it comes to preparedness for a privacy-related crisis. Only 50% of Canadian companies and 44% of American companies have a crisis management process. Much work has to be done in both countries in this area.

Also, less than half of the respondents in each country perform privacy monitoring on a regular basis. Similar numbers are reported when examining the monitoring of internal compliance with a company's own privacy policy. Significant improvement will have to be shown in these areas, if the regulatory environment continues on its path of enforcing privacy.

Benchmark Six: Choice and Consent

How do companies in each country manage the privacy preferences of their constituents? Most Canadian and American companies are sharing customer-centric information with *affiliate* companies; however, more American companies (76%) report that they are sharing customer-centric information with *third parties*, than Canadian companies (47%) are doing.

Also, 26% more Canadian companies provide opt-out choices of secondary use or sharing of personal information (79% Canadian to 53% American). Still, only 50% of Canadian companies have flexibility (defined as multiple channels or methods) to express their privacy preference.

With respect to employees, 44% of U.S. companies and 72% of Canadian ones provide choice over the way employee personal information is used (which includes sharing among affiliates and third parties).

Benchmark Seven: Global Standards

More Canadian companies make global privacy standards a priority than U.S. companies do. Over 79% of Canadian companies state that they are in substantial compliance with European Union privacy/data protection laws (also known as Safe Harbor Laws). Only 33% of American companies are in compliance with them.

The European Community laws are very important within the community, so much so that data will not be transported to a jurisdiction that does not comply with minimum privacy principles. Privacy concerns have created, in this way, a very real non-tariff trade barrier. Thus, concerns about and respect for these laws should be a genuine concern for any forward-looking business leader.

Twice as many Canadian companies as U.S. companies monitor national privacy practices, laws and regulations. Also, more Canadian companies (63%) evaluate trans-border data flows than do U.S. firms (44%).

Benchmark Eight: Redress

A final fascinating basis of comparison is that of redress for corporate constituents. Programs designed to respond to privacy complaints aid companies helping them reduce the likelihood of *public* privacy-related crisis and to redress attendant problems.

Again, Canadian companies appear to be more advanced. Canadian company constituents can access and correct their personal information 71% of the time, compared to 25% in the U.S. context. A redress process is more likely to be described in a Canadian privacy policy (61%) than in an American one (31%). Most American *employees* have access to their personal information, while all Canadian employees have that access.

As to having formal processes for enforcing privacy violations, Canadian companies are much more likely to have one (61%), compared to American companies (19%). Interestingly, though, neither country has a high percentage of a redress process having specific reporting requirements to management (Canada-38%, U.S. – 21%).

Some Conclusions

It would appear that on the basis of this small sample of large Canadian and American public companies, that the Canadian companies outperform their American counterparts in most areas of comparison, with the exception of protection against external penetrations for data. Perhaps, more importantly, though, it is important to note that *both countries* have a great deal of room for improvement of their processes and practices with respect to the collection, use, storage and disposal of personal information. The relative newness of comprehensive legislation in both countries is certainly one factor (for example, Canada's *Personal Information Protection and Electronic Documents Act* has only been phased-in since January of 2001; Ontario's *Health Information Protection Act, 2004* is only to become law in November). Making privacy a central business concern, perhaps as part of an overall corporate governance imperative, with responsibility flowing to a senior executive, is not yet a reality in either country. Conducting regular, in-house privacy audits, education of management and staff as to privacy laws and requirements, as well as determining client/customer/employee preferences and incorporating them into corporate policy is a growing phenomenon, but is not at all reality, either. As laws continue to develop, both countries will continue to experience growing pains. Monitoring of the changing regulatory environment, analysis of the changing legal landscape, both nationally and internationally, will have to be enhanced. Canadians and Americans, both, put a high value on their privacy. The businesses that service them in every country will have to become more compliant with these privacy laws and more sensitive to the concerns about the value of sensitive personal information.