

Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?

EXECUTIVE SUMMARY

The *Personal Information Protection and Electronic Documents Act* (“*PIPEDA*”) was introduced in 2001 to protect Canadians from inappropriate collection, use and disclosure of their personal data by organizations in the course of commercial activities. Five years later, it is not clear to what extent organizations are in fact respecting the legislation. This study was designed to shed some light on that question, by assessing the compliance of retailers with certain key provisions of *PIPEDA*.

We assessed the compliance of 64 online retailers with the *PIPEDA* requirements for openness, accountability and consent. We also assessed the compliance of 72 online and offline retailers with the *PIPEDA* requirement for individual access. The results of our assessment indicate widespread non-compliance in all four areas.

While almost all companies we assessed had a privacy policy and were thus aware of the need to respect customer privacy, many failed to fulfill even basic statutory requirements such as providing contact information for their privacy officers, clearly stating what they do with consumers’ personal information, and responding to access to information requests. A significant proportion of the policies we examined were unclear on key points such as whether or not consumer information is shared with other companies. Many failed to provide a clear and conspicuous method for consumers to opt-out of unnecessary uses and disclosures of their personal information, often relying on a clause buried deep in a lengthy privacy policy that consumers are unlikely to review.

A number of policies we examined were misleading, suggesting for example that no secondary use or sharing of personal information would take place without the consumer’s explicit consent, but then assuming such consent unless the consumer exercised an often inconspicuous or incomplete opt-out.

The following are key findings from the compliance assessments:

General Practices

- Almost all online retailers have privacy policies (94% of our sample), and most post them on their websites (92%).
- Privacy policies tend to be lengthy: 63% of those in our sample were over 1000 words long, and 35% were over 2000 words long.
- The vast majority of online retailers (at least 93% of our sample) use personal consumer information (“consumer information”) for their own marketing purposes.

- A large proportion of online retailers (1/2 to 2/3 of our sample) share consumer information with other companies for purposes beyond those necessary for the transaction or service in question. Only one-third of our sample stated that they do not do so.
- Only one of the 29 companies in our sample that admitted to sharing consumer information with other organizations, restricted its data-sharing to affiliates.
- A large majority of retailers (78% of our sample) rely on opt-out methods to obtain consumer consent to secondary uses or disclosures of their personal information.

Principle 4.1 – Accountability

- Online retailers are doing a poor job of ensuring that front-line staff are aware of the existence of the privacy policy, know who is responsible for it, and can direct inquirers to both the policy and the responsible officer. 68% of companies we contacted took over five minutes, and 22% took over ten minutes, to answer the questions: “Do you have a privacy policy?”, “How can I get it?” and “Who in your company is responsible for privacy matters?”
- 56% of companies we contacted by phone could not provide the name of an individual responsible for privacy when asked. Moreover, 30% of privacy policies we reviewed did not provide contact information for a person responsible for compliance with the policy.
- Few of the retailers we tested (only 14%) provided consistent contact information for designated privacy officers in their privacy policies and over the phone.

Principle 4.8 - Openness

- It is unreasonably difficult for consumers to acquire information over the phone about companies’ policies and practices with respect to the management of personal information. As noted above, 68% of companies we contacted took over five minutes, and 22% took over ten minutes, to answer the questions: “Do you have a privacy policy?”, “How can I get it?” and “Who in your company is responsible for privacy matters?”
- Four companies (6%) in our sample had no privacy policy whatsoever.
- While most online retailers make their privacy policies accessible online, 63% of companies in our sample could not or would not provide a copy by mail, fax or email when requested to do so.
- A significant proportion of privacy policies fail the test of clarity, even when tested by people with university education. Although 87% of policies reviewed were considered “generally understandable” by Assessors, many fewer were found to be clear on key points once Assessors looked more closely. Specifically, Assessors found that companies were unclear about the purpose of collection in

22% of cases, about what personal information they collect in 27% of cases, about how they use the information in 30% of cases, and about to whom they disclose the information in 45% of cases.

- An even higher proportion of privacy policies were incomplete:
 - 30% did not provide contact information for a privacy officer;
 - 38% made no reference to the consumer's right to access his or her personal information held by the company;
 - 27% did not describe the type of consumer information held by the company;
 - 18% did not describe what the company does with consumer information;
 - 34% of those that admitted to sharing consumer information with other organizations did not describe the type of information that they share;
 - 86% of those that admitted to sharing did not indicate with whom they share consumer information; and the remaining 14% provided examples only.

Principle 4.3 – Consent

- Not surprisingly, the vast majority of online retailers we surveyed (78%) rely on opt-out methods, at least in part, to obtain consumer consent for secondary uses and disclosures of their personal information. Only 8% use opt-in methods exclusively, and a surprising 14% do not bother to get consent through any means when customers register or order on their site, even though they admit to secondary uses or disclosures or are unclear on this point.
- Under *PIPEDA*, consent must be informed. Yet, 17% of the privacy policies reviewed were unclear about whether the company uses consumer information for marketing purposes, and 18% were unclear about whether the company shares consumer information with other companies. A further 6% of companies did not have privacy policies at all. In 31% of the cases we reviewed, the companies provided no notice via the privacy policy or otherwise during the registration or ordering process.
- Moreover, during the registration or ordering process, the majority of the 64 companies we assessed (53%) provided notice to customers only via a link to the privacy policy, requiring consumers to visit the privacy policy and read through it for an understanding of what the company does with their personal information. Of these, 56% failed to bring the link to the privacy policy to the customer's attention during the registration or ordering process.
- We found a number of misleading privacy policies. In particular, of the 60 privacy policies assessed, 18% suggest that the company uses opt-in consent when in fact it relies on opt-out consent. This misleads consumers into thinking that their information will not be used for secondary purposes when in fact it will.

- Twenty-nine companies (48% of our sample) admitted to sharing consumer information with other companies for purposes other than the transaction in question (another 11 (18%) were unclear). Yet, ten of these companies (34% of those that clearly share) did not offer consumers a choice regarding this practice during the registration or ordering process.
- The methods used by many online retailers to obtain consent from consumers do not meet the requirements for valid consent.
 - Of those companies relying on opt-out consent, 50% did so merely via a link to an often lengthy privacy policy as part of the registration or ordering process. In these cases, the majority (52%) failed to bring the link to the privacy policy to the customer’s attention.
 - Of those companies that included an opt-out in their privacy policy, 60% buried it inconspicuously in the often lengthy policy.
 - Ten companies in our sample offered fewer opt-out options during the registration or ordering process than via their privacy policies, without any indication to consumers that additional opt-out options were available via the privacy policy. This misleading practice was exacerbated by the fact that none of these companies bothered to bring their privacy policy to the attention of consumers during the registration or ordering process.
 - Of those companies relying on opt-out consent, 50% did not offer an immediate opt-out option as part of the transaction; rather, consumers have to consent against their will initially and then take additional steps to opt-out.
- In seven cases (11%), the retailer clearly required consent to a secondary purpose in order for the consumer to transact. In none of these cases did the consumer receive any value in exchange for such consent. In an additional 18 cases, Assessors were not sure whether consent to a secondary use or disclosure was mandatory, due to lack of clarity in the privacy policy or an absence of a written privacy policy. Thus, potentially 39% of companies we assessed are violating *PIPEDA*’s “refusal to deal” section.

Principle 4.9 – Individual Access

- A large proportion of companies are failing to comply with the *PIPEDA* requirement to inform individuals of the existence, use and disclosure of their personal information upon request, and to give individuals access to that information.
- One-third (35%) of the companies we tested did not respond at all to access requests.
- Of the companies that did respond,
 - 42% failed to provide details about the Requestor’s personal information they had on file;

- 37% provided no account or an inadequate account of how they use the personal information; and
- 58% did not give a list of companies to whom they have or may have disclosed personal information about the Requestor;

despite being specifically asked for this information by the Requestor.