BLG

U.S. Perspectives from Canada's Law Firm

Canadian privacy law – What U.S. businesses need to know

If you are a consumer-facing business in the United States, or are in the business of advising them on privacy matters, you have probably put significant effort and resources toward complying with the *California Consumer Protection Act* (CCPA).

You could be looking to leverage some of these efforts to comply with Canadian privacy laws, especially given the prospect of privacy law reform at the federal level and in Québec. If so, the first important distinction between U.S. and Canadian approaches to privacy is that the principle-based approach in Canadian privacy law contrasts with the CCPA's prescriptive and detailed requirements. This is often surprising to U.S. businesses.

Canadian privacy law has a strong focus on consent, imposes data minimization and reasonableness standards for any data-handling practices, and includes certain restrictions on cross-border data transfers. Canadian breach reporting requirements also have a much broader scope than those in the U.S.

Privacy law in Canada

As opposed to the U.S., businesses operating in all Canadian provinces and territories are subject to a comprehensive privacy statute. At the federal level is the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA regulates how private sector organizations collect, use and disclose personal information about individuals in the course of commercial activities. It applies in all provinces that have not adopted a substantially similar law, and to organizations that transfer personal information across national and international borders. The provinces of Alberta (*Personal Information Protection Act*), British Columbia (*Personal Information Protection Act*) and Québec (*Act respecting the protection of personal information in the private sector*) have adopted substantially similar laws.

In an employment setting, PIPEDA only applies to federally-regulated businesses (banks, airlines, railway companies, *etc.*).

Notices and privacy policies are important, but consent remains key

The CCPA includes specific requirements about the notices businesses must provide to consumers. While transparency is an important principle under Canadian privacy laws, Canada does not require a similar level of detail. Rather, Canadian privacy laws put strong emphasis on consent. Individuals have the right to withdraw consent, and not only with respect to the "sale" of their personal information.

Generally speaking, certain situations warrant express consent, namely:

- when the information involved is sensitive;
- when the processing of personal information is outside the individual's reasonable expectations; or
- when information sharing creates a meaningful residual risk of significant harm to the individual.

Further, organizations must give individuals the choice to refuse any collection, use or disclosure of personal information that is not "integral" to the services the organization is providing. This may include using personal information internally for marketing purposes.

Organizations doing business in Canada need to navigate the various exceptions to the aforementioned consent principle. One of the most important exceptions applies in the employment context. Generally, an organization may collect, use, or disclose personal information if reasonable/necessary to establish, manage or terminate the employment relationship, as long as the organization lets the individual know of such purposes. Exceptions vary between PIPEDA and the three provincial laws. For instance, there is no employment exception under Québec law.

Businesses must be mindful of data minimization and reasonableness

Similar to the European Union's General Data Protection Regulation (GDPR), "data minimization" is a core principle of Canadian privacy law. This concept is generally absent in U.S. privacy law. Generally, it means that businesses must limit the collection of personal information to what is necessary for the legitimate purposes it has identified, and may not use or disclose it for other purposes. Organizations must also have retention policies in place to ensure that personal information is only retained as long as necessary to fulfil these purposes.

Another important requirement under Canadian law is the "reasonableness standard." More specifically, Canadian privacy laws provide that organizations may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate under the circumstances. This requirement applies regardless of consent. It often comes up in surveillance scenarios involving employees and with respect to innovative marketing initiatives.

To determine if a practice is reasonable, privacy regulators use a four-part test centred on necessity and proportionality. More specifically, the organization should be able to demonstrate that:

- the organization's purpose represents a legitimate need/*bona fide* business interest;
- the process would be effective in meeting this need;
- there aren't any less-invasive ways to achieve the same ends at comparable cost and with comparable benefits; and
- the loss of privacy is proportional to the benefits.

Privacy regulators generally expect organizations to conduct a privacy impact assessment (PIA) when a new data-handling practice could raise concerns in this respect.

Cross-border transfers and intra-company sharing agreements

U.S. privacy laws do not include restrictions on the cross-border transfers of personal information. While Canadian privacy laws are not as stringent as the GDPR in this respect, U.S. businesses should be aware of the requirements they must follow before importing personal information of their Canadian customers or employees to the U.S.

First, organizations must inform Canadian customers or employees that their personal information will be transferred outside of Canada and that, as a result, their personal information will be subject to the laws applicable in these foreign jurisdictions and potentially made available to foreign government authorities. This is generally done through a statement to that effect in the organization's privacy policy.

Second, pursuant to Canadian privacy law's "accountability" principle, organizations must ensure that personal information collected in Canada is adequately protected when transferred to a third party for processing, including when it is transferred to an affiliated party (*e.g.* the Canadian entity's parent company) in a foreign jurisdiction (see PIPEDA Report of Findings #2019-001). Unless the personal information being handled is of limited scope and sensitivity and the foreign entity is subject to pre-existing policies and practices adequate under PIPEDA, organizations must enter a formal written arrangement between the entities, which should generally include details about the following:

- what personal information is being handled by the foreign entity, including both information shared by the Canadian organization and any information collected directly by the foreign entity on behalf of the Canadian entity;
- what specific rules, regulations and standards need to be complied with in handling the information, including PIPEDA;
- the roles and responsibilities of key stakeholders within both entities for handling personal information, including responsibilities for specific functions, decision-making, safeguards and breach response;
- information security obligations;
- acceptable uses of information;
- retention and destruction obligations; and
- reporting and oversight arrangements to ensure compliance with the above, including reporting obligations in the case of a breach that could compromise the personal information.

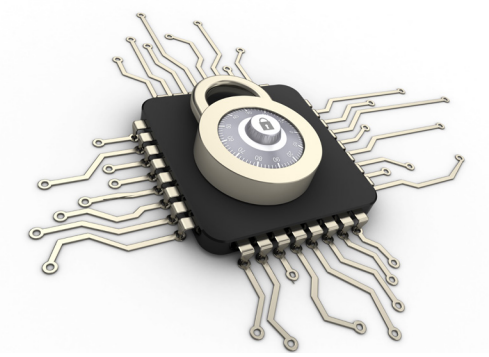
If the U.S. entity does not have policies and procedures specifically tailored to PIPEDA and when personal information collected in Canada is transferred to the U.S. as part of the organization's regular operations, it is recommended to adopt an agreement that complies with these requirements.

Breach reporting – A reportable breach does not have to involve specific data elements

All U.S. states have adopted security breach reporting requirements, which are triggered when a combination of specific categories of personal information are compromised. Generally, in order to trigger an obligation to report a breach, sensitive information, such as government identification numbers or health-related data, must be compromised.

Canadian privacy laws take a different approach: a breach will generally be reportable if there is unauthorized access to or disclosure that creates a "real risk of significant harm" to the affected individuals. Note that British Columbia and Québec have not yet adopted breach reporting requirements, although regulators in both provinces recommend voluntary reporting. In June 2020, the Québec government proposed a privacy law reform that would introduce mandatory breach reporting.

The "real risk of significant harm assessment" takes into account the sensitivity of the information and the probability of misuse. The federal Privacy Commissioner issued guidance to help organizations evaluate these factors. Of note, sensitive information is not limited to information that may lead to fraud or identity theft, but includes information that may cause humiliation and embarrassment. The Alberta Office of the Information and Privacy Commissioner has taken the position that breaches involving contact information that could be used for phishing attacks meet the real risk of significant harm threshold.



Conclusion – Will Canada see FTC-type privacy enforcement?

Unlike the U.S. Federal Trade Commission (FTC), Canada's competition regulator (the Competition Bureau) has not historically played a role in privacy enforcement. Privacy regulators do not have strong enforcement powers under Canadian privacy laws. As of now in Canada, the main financial threat for businesses on the privacy front has come from class actions (to date none have been heard on their merits; however, plaintiffs have obtained significant settlements).

The situation may change following eventual federal privacy law reform. In December 2019, the Prime Minister's mandate letters to the Minister of Justice of Canada refer to a reform of PIPEDA that will give the federal Privacy Commissioner enhanced powers. In the June 2020 privacy bill introduced by the Government of Québec, the privacy regulator would have powers to impose administrative monetary penalties of up to C$10,000,000 or, if greater, the amount corresponding to 2 per cent of worldwide turnover in the preceding year.

Finally, the Competition Bureau recently concluded its first privacy-related settlement. Facebook Inc. agreed to pay a C$9 million penalty (approximately US$6.7 million) after the Competition Bureau concluded that the company made false or misleading claims about the privacy of Canadians' personal information on Facebook and Facebook Messenger.

These developments may result in greater financial risk relating to privacy for businesses operating in Canada.

Calgary
Centennial Place, East Tower
520 3rd Ave S W, Suite 1900
Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza
100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400
Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre
200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com

Author

François Joli-Coeur
T 514.954.3144
FJolicoeur@blg.com

Printed in Canada. BD9748 – 08 – 20

Borden Ladner Gervais