# CANADA'S CRACK DOWN ON DATA PRIVACY AND WHAT THIS COULD MEAN FOR INTERNATIONAL BUSINESS

**Erin Schachter** Therrien Couture Joli-Cœur LLP

With many individuals working from home, cyberattacks of all kinds are on the rise. Ransomware, data leaks, identity theft, fraud, and the unauthorized collection and resale of personal information, are all buzzwords that quickly gain enormous media attention during the chaos of 2020. Individuals are beginning to speak out against the use of their information by corporations and many countries are beginning to listen. Significant policy changes are occurring on a global level and Canada is neither the first nor the last to strengthen its domestic policy.

Incorporeal goods, such as data, are notoriously difficult to keep within the bounds of one nation. Consequently, changes to the privacy practices of one country can have tremendous influence on an international scale.

In Canada, the federal and provincial governments have begun to take concrete efforts to strengthen their legislation governing how businesses handle personal data. Many have noted that Canada is following the stricter enforcement trend initiated by the European Union and found in the *General Data Protection Regulation* ("GDPR")[1].

The GDPR was adopted on April 14, 2016, and became applicable starting on May 25, 2018. The Regulation was very innovative at the time and, after its adoption, it became a model for many national laws outside the European Union. It appears that Canada and some of its provinces are now following in the footsteps of the GDPR with the new legislation it adopted at the end of 2020.

Canada has two federal privacy laws that are enforced by the Office of the Privacy Commissioner of Canada. The *Privacy Act*[2] regulates how the federal government handles personal information, whereas the *Personal Information Protection and Electronic Documents Act*[3] (PIPEDA) controls how businesses handle personal information.

PIPEDA applies across Canada but is pre-empted by privacy legislation enacted by a province if that legislation is substantially similar[4]. Of Canada's 10 provinces and three territories, only three provinces have opted to enact or maintain their own privacy legislation (Alberta, British Columbia, and Quebec). Federally regulated businesses that conduct business in Canada are always subject to PIPEDA regardless of their location in Canada. Furthermore, information that crosses provincial or national borders in Canada is subject to PIPEDA regardless of where the business is located.

For this reason, changes to privacy legislation at the federal level have an enormous impact on business across Canada. Currently, both the federal government and the provincial government in the province of Quebec are implementing new rules.

In Canada, in November 2020, Parliament approved Bill C-11, *An Act to Enact the Consumer Privacy Act and the Personal Information Protection and Data Protection Tribunal Act and to make consequential and related amendments to other Acts* ("Bill C-11").

In Quebec, in June 2020 the National Assembly approved Bill 64, *An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information* ("Bill 64")[5].

If passed, these Bills will strengthen the protection of personal information collected by private institutions. Even if these Bills are not passed "as is," we can expect a number of these measures to be enacted in the coming years.

These Bills include the following measures:

- Stricter restrictions on consent to the use of an individual's personal information, and a guarantee that the information will only be used for the intended purpose.
- Stricter requirements regarding the wording of the request for consent, which must be written in a manner that is easy to understand.
- Special rules regarding consent when dealing with "sensitive" information. Information is designated as "sensitive" if, because of its nature or the context of its use or dissemination, it involves a high level of reasonable expectation of privacy.
- The requirement to appoint an individual within the organization who will be responsible for compliance with applicable legislation.
- Enhanced rights are given to individuals to determine how their information is handled and whether they want their information destroyed or no longer disseminated. These rights differ according to the proposed legislation.

Another important element is the new restriction on data transfers between jurisdictions. The provincial legislation requires additional measures when seeking to transfer data out of the province. An assessment of the protection afforded must be made to determine whether the exported data will benefit from a similar level of protection as the domestic data. If it is determined that the destination of the potential transfer does not provide an equivalent level of protection, the transfer of the data will be prohibited. Where transfers are allowed following the assessment, they must be accompanied by a written agreement between the parties.

This requirement is much stricter than under federal legislation, which provides for a general obligation to use agreements or other methods to ensure comparable levels of protection for information transferred to third parties, without necessarily conducting a preliminary assessment.

In both cases, if foreign jurisdictions do not have adequate safeguards in place, it will be necessary to put in place rigorous contracts to ensure the protection of information. Otherwise, the company that transferred the information could be held liable in the event of an incident or a breach. Key point: if you want to do business in Canada or with Canadians, you may be required to conform to Canadian privacy standards.

Overall, these Bills provide for more stringent legislation on the handling of personal information, greater responsibility on the part of businesses, greater control mechanisms on the part of regulatory authorities in the event of an incident, as well as stricter penalties for businesses that do not comply with the law.

The sanctions proposed in the Bills far exceed those that existed before. If the Bills are adopted, companies could be fined between $10 million and $25 million or a percentage of their revenues. These sanctions are similar to the GDPR, which sets a maximum fine of €20 million or 4% of annual worldwide turnover for infringement. These percentages and the way they are calculated differ. In the proposed provincial legislation, the amount is between 2% and 4% of the company's annual revenues, while in the proposed federal legislation, the amount is between 3% and 5%.

By comparison, in the United States, various levels of regulators may issue penalties, but there is no unified legislation or authority throughout the United States thus penalties can vary widely.

As many countries, including Canada, are adapting their legislation to keep pace with trends in the GDPR, one of the lingering questions is whether this will have an impact on the United States.

Businesses today are highly dependent on technology, and even more so since the global pandemic. Personal information is ubiquitous, and few businesses can operate without it. Authorities in Canada are committed to restricting the use and handling of personal information. The consequences of not complying with these new restrictions once they take effect could be devastating for businesses.

*Erin Schachter of Therrien Couture Joli-Cœur LLP is an attorney operating in the field of intellectual property law, technology law, data privacy as well as other commercial litigation matters. Erin is a member of the litigation team, and acts on behalf of clients on a national and international level before the provincial and federal courts in Quebec.*

1 *Regulation (EU) 2016/679.*
2 *Privacy Act* R.S.C., 1985, c. P-21
3 *Personal Information Protection and Electronic Documents Act* S.C. 2000, c. 5
4 Organizations in the Province of Quebec Exemption Order (SOR/2003-374)
5 Bill C-11 and Bill 64 are collectively referred to as the Bills