Canada: Recent developments in Canada's privacy landscape

By **Antoine Aylwin** Partner
aaylwin@fasken.com
Fasken, Montréal

By **Iara Griffith** Lawyer
igriffith@fasken.com
Fasken, Montréal

No longer a by-product of business operations, personal information has become a resource to be mined, processed, analysed, shared, and sold. In 2018, the adoption of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') sparked a worldwide legislative flurry. It pushed countries to revamp their privacy laws to keep up with these new standards. Here's how Canadian provinces and the federal government caught the wave.

Quebec's privacy legislation grew some teeth

In June 2020, Quebec was the first province to introduce the Act to modernize legislative provisions as regards the protection of personal information ('Bill 64') to overhaul its privacy legislation. Bill 64[1] was adopted in September 2021 and amends some 20 statutes, including the province's public and private sector laws. While Bill 64 provisions enter into force between 2022 and 2024, most of its provisions take effect on 22 September 2023. Key provisions include the appointment of a privacy officer, mandatory reporting of confidentiality incidents, privacy impact assessments, and privacy notices written in plain language.

As per Quebec's Minister Responsible for Access to Information and the Protection of Personal Information, Bill 64 'has teeth': administrative penalties go up to CAD 10 million (approx. €6.8 million) or 2% of the previous year's worldwide turnover, whichever is greater. Penal fines go up to CAD 25 million (approx. €17.2 million) or 4% of the previous fiscal year's worldwide turnover, whichever is greater.

Quebec looks to catch up on health information

Quebec also introduced[2] An Act respecting health and social services information and amending various legislative provisions ('Bill 19') in December 2021. If enacted, it will encompass all health information held by health institutions, excluding information collected for human resource management purposes concerning members of staff or professionals.

What is health information?

Health information is defined as any information about an individual, whether identifiable or not, that relates to one or more of the following:

- a person's physical or mental health status and their determinants, including a medical or family history;
- any material collected to assess or treat a person, including biological material or aid that compensates for disability;
- health or social services provided

to a person, including the nature of the services, results, where services were provided and the service provider;
- information obtained while performing a function under the Public Health Act; and
- any other characteristic determined by government regulation.

Under Bill 19, personal information is considered health information when combined with other health information (e.g., a name attached to a lab test result). Bill 19, which will apply to various health bodies, will also bind all individuals or entities that enter an agreement with a health institution to provide health or social services on the organisation's behalf, and any other person, partnership, or organisation determined by regulation.

What this means in terms of governance

Health institutions must take reasonable measures to protect health information and ensure its accuracy. They must comply with the Health Minister's governance rules and adopt governance policies that establish the following:

- the roles and responsibilities of the institution's staff and professionals with regard to health information throughout its life cycle;
- the categories of persons who may, in the exercise of their functions, access health information;
- logging mechanisms and security measures;
- an updated list of the technological products or services in use;
- a procedure for processing confidentiality incidents;
- a procedure for processing complaints; and
- a description of the training and awareness activities offered regarding health information.

How Bill 19 and 64 intertwine

Bill 19 incorporates several of Bill 64's key measures, such as the designation of a health information privacy officer, the carrying out of privacy impact assessments, mandatory reporting of confidentiality incidents, transparency requirements, and individuals' rights.

Offences

Bill 19 provides for two categories of penal sanctions. The less serious offences are punishable by a maximum fine of CAD10,000 (approx. €6,890) for individuals, and CAD 30,000 (approx. €20,670) in other cases. The most serious offences are punishable by a maximum fine of CAD100,000 (approx. €68,910) for individuals and CAD150,000 (approx. €100,360) in other cases. Penal actions are prescribed up to five years after the commission of the offence.

One ID for all and a new minister

As is the case in several provinces, Quebec is considering creating a digital identifier to facilitate access to certain government services. While such a tool offers practicality, it also poses significant security challenges. Given the prevalence of cyberthreats, governments must spare no effort to ensure that they have sufficient resources in place before moving forward with such an initiative. Taking a step in that direction, the Government of Quebec recently announced the creation of a cybersecurity ministry.

New year, new federal bill?

In November 2020, the Government of Canada tabled Bill C-11, the Digital Charter Implementation Act. In doing so, it hoped to modernise the federal personal information protection regime. Bill C-11 promised major reforms to Canada's Personal Information Protection and Electronic Documents Act ('PIPEDA'). However, in May 2021[3], Canada's Privacy Commissioner ('the Commissioner') harshly criticised the bill, calling it a 'step back overall'.

The Commissioner noted that the Bill C-11 is often misaligned and offers consumers less protection than laws elsewhere. He recommended a framework that would entrench privacy as a human right rather than prioritising commercial interests. He also suggested that Bill C-11 weakens existing accountability provisions by favouring self-regulation. While the Bill C-11 seeks to provide greater flexibility through new exceptions to consent, he contended that certain exceptions were 'too broad or ill-defined to promote responsible innovation.' Exceptions to consent should be based on legitimate business interests as part of a rights-based approach.

The Commissioner also highlighted the importance of maintaining Canada's adequacy status under the GDPR and decried the number of privacy violations not subject to sanctions. While enabling the Office of Privacy Commissioner of Canada to recommend high monetary penalties, the new provisions have important limitations, including an administrative appeal that delays consumers' access to justice.

In December 2021, the Minister of Innovation announced that he would introduce an amended bill in 2022.

Ontario joins private sector privacy realm

In June 2021, the Government of Ontario published a white paper[4] ('the White Paper') titled Modernizing privacy in Ontario. It intended to make Ontario 'the world's most advanced digital jurisdiction.' Objectives included implementing a fundamental right to privacy for Ontarians and additional safeguards for artificial intelligence technologies. The Ontarian Government also planned to update consent rules, promote responsible innovation, and correct systemic power imbalances between individuals and organisations.

Key areas of reform included:

- a rights-based approach to privacy;
- safe use of automated decision-making;
- enhanced consent;
- transparency; and
- dedicated protections for children.

On 7 September 2021, Ontario's Information and Privacy Commissioner ('IPC') commented[5] on the White Paper. At the outset, she stressed the importance of moving forward with the reform regardless of whether the Federal Government amends or replaces Bill C-11. She recommended adding principles of transparency and accountability to the preamble, tightening exceptions to prohibitions on automated decisions, clarifying disclosure requirements for implied consent, ensuring interoperability and data portability rights, and including the requirement to inform individuals of their right to withdraw consent. In general, the IPC welcomed the Ontarian Government's proposals.

The IPC suggested adding certain offences and extending the application of offences to individuals, not just organisations, as other jurisdictions have done.

Finally, the IPC noted that the White Paper had not raised important points regarding mandatory breach notification, definition and application of provisions, retention of personal information, and transitory provisions.

How British Columbia amended its public sector law

In November 2021, British Columbia ('BC') enacted Bill 22[6], which significantly changes the Freedom of Information and Protection of Privacy Act ('FIPPA'). FIPPA defines how public bodies in BC collect, use, disclose, and retain personal information.

Data residency

With respect to data residency, public bodies may now disclose personal information outside Canada subject to applicable regulations. These changes 'help public bodies keep pace with new technology and provide the services people expect in a modern age,' explained the Minister of Citizens' Services.

Breach notification

Bill 22 also provides for mandatory breach notification where a breach poses a risk of significant harm, thus aligning with similar obligations under other provinces' public sector privacy laws. The new FIPPA broadly defines 'significant harm' as including identity theft, significant humiliation, significant damage to reputation or relationships, significant loss of employment, business or professional opportunities, significant financial loss, and significant negative impact on a credit record.

Offences

Bill 22 adds new privacy offences to FIPPA, including offences relating to the unauthorised collection, use, or disclosure of personal information and a failure to report unauthorised disclosures of personal information.

A person convicted of committing a privacy offence is liable to a fine of up to CAD 50,000 (approx. €34,470); the fine goes up to CAD 500,000 (approx. €344,680) for corporations. Service providers and their employees and associates may present a due diligence defence.

BC plans to modernise its private sector law

BC's Personal Information Protection Act ('PIPA') outlines how organisations may collect, use, and disclose personal information. Every six years, a Special Committee undertakes a comprehensive review of the PIPA to determine its effectiveness in the current social and economic environment. The Special Committee published its report[7] in December 2021.

Key recommendations included the following:

- harmonisation of PIPA and FIPPA;
- ensuring that PIPA meets GDPR and anticipated federal requirements;
- updating requirements of explicit consent to include meaningful consent provisions;
- defining new sensitive categories of information which would require explicit consent;
- adopting Privacy by Design principles;
- strengthening provisions regarding access requests;
- ensuring data portability;
- requiring organisations to clearly outline retention periods and methods of data destruction in their privacy policies;
- mandatory privacy impact assessments;
- mandatory breach notification; and
- increased investigative and punitive powers to BC's Office of the Information and Privacy Commissioner.

Final thoughts

Canada's Privacy Commissioner recently noted[8] that our federal privacy laws do not adequately protect Canadians' fundamental rights and core values. While three provinces have already proposed frameworks that reconcile digital innovation and privacy as a fundamental right, a new federal law is highly anticipated. What's more, the harmonisation of various laws is paramount where physical boundaries no longer limit business activities. Companies want to comply with new requirements, but they need consistent rules to do so. As such, Canada and its provinces should work together to meet this need.

1. *See: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2021C25A.PDF*
2. *See: http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-19-42-2.html*
3. *See: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/*
4. *See: https://www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49462*
5. *See: https://www.ipc.on.ca/wp-content/uploads/2021/09/2021-09-03-ipc-comments-on-gov-white-paper_modernizing-privacy-in-ontario.pdf*
6. *See: https://www.leg.bc.ca/content/data%20-%20ldp/Pages/42nd2nd/1st_read/PDF/gov22-1.pdf*
7. *See: https://www.leg.bc.ca/content/CommitteeDocuments/42nd-parliament/2nd-session/pipa/report/SCPIPA-Report_2021-12-06.pdf*
8. *See: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/ar_202021/*