OSLER

The freight train of privacy legislative reform keeps rolling

JANUARY 11, 2023 11 MIN READ

Related Expertise

- Privacy and Data Management

Authors: Adam Kardash, Colleen Morawetz, Maryna Polataiko

Over the past year, legislative reform has continued to be the focal point in the highly dynamic Canadian privacy arena. The first phase of the reformed privacy legislative scheme in Québec came into force, with security breach notification obligations and certain other new compliance obligations for companies becoming effective in September 2022. In September 2023, the majority of the amendments to Québec's legislative scheme will come into force, including an enforcement regime with potentially severe financial penalties.

Additionally, in 2022, the federal government re-introduced a new private sector privacy law framework. If passed, the framework will also expose companies across Canada to severe financial penalties for privacy breaches, enhanced litigation risk and significant compliance costs.

It is more important than ever for companies doing business both in Québec and across Canada to have a thorough understanding of their personal information practices and their privacy obligations. Companies will need to identify and mitigate the expanding array of privacy, legal and reputational risks associated with the collection, use and disclosure, as well as other processing, of personal information.

Other new federal bills introduced over the past year include statutory frameworks governing artificial intelligence systems and critical infrastructure cybersecurity. Legislative reform momentum has varied among other Canadian jurisdictions.

Québec: Parts of Bill 64 come into force

The first wave of amendments under Québec's Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* [PDF], came into force on September 22, 2022. While new penalty provisions do not take effect until 2023, companies carrying on business in Québec are now subject to a number of new requirements.

In particular, the individual who has the "highest authority" in an organization is recognized as the person in charge of the protection of personal information, unless they delegate the responsibility in writing to another person within the organization. Additionally, an organization must report "confidentiality incidents" presenting a risk of serious injury to affected individuals to the Commission d'accès à l'information (CAI) and those affected individuals. The organization must also keep a record of all confidentiality incidents.

Bill 64 amends the *Act to establish a legal framework for information technology* by requiring organizations to disclose to the CAI any process involving the recording of biometric characteristics to verify or confirm a person's identity. The organization must notify the CAI at least 60 days in advance of the creation of a database of biometric characteristics.

Finally, an organization may now communicate personal information without consent, under prescribed conditions, including where it is necessary to conclude a commercial transaction or where the communication is to a recipient wishing to use the information for study, research or statistical purposes.

With the exception of data portability provisions, the balance of amendments introduced by Bill 64 come into force in September 2023. Among these are the penalty provisions. Failure to comply with the *Act respecting the protection of personal information in the private sector* will expose organizations to fines of up to the greater of $25 million and the amount corresponding to 4% of worldwide turnover for the preceding fiscal year. Organizations can also be exposed to administrative monetary penalties of up to the greater of $10 million and the amount corresponding to 2% of worldwide turnover for the preceding fiscal year.

In addition, organizations will be required to create an internal policy suite to address the lifecycle of personal information in their custody and control. Organizations will also be required to conduct privacy impact assessments for any project involving the acquisition, development or overhaul of an information system or electronic service delivery system that entails the processing of personal information.

Bill 64 strengthens consent requirements and creates new exceptions to consent for personal information processing. Organizations will need to examine all collections, uses and disclosures of personal information, improve their consent notices, develop or enhance consent management practices and otherwise ensure the lawful processing of personal information.

Under the novel "confidentiality by default" requirement, organizations must implement the "highest level" of confidentiality by default with respect to public-facing products or services. Finally, organizations collecting personal information from individuals using technology that allows those individuals to be identified, located or profiled must first inform the individual of such technology and of the means available to activate such functions.

Once data localization restrictions are in effect, organizations will have to create an inventory of all cross-border disclosures and transfers, including transfers of personal information to other Canadian provinces. Organizations will be required to conduct a privacy impact assessment prior to any disclosure of personal information outside Québec to ensure that the personal information will be "adequately protected" in the other jurisdictions. Organizations will be prohibited from transferring or disclosing personal information outside the province of Québec in circumstances where such information will not receive "adequate protection." This will be determined in light of "generally recognized principles regarding the protection of personal information."

Federal: Sweeping legislative reform introduced

In June 2022, the Government of Canada tabled Bill C-27, the *Digital Charter Implementation Act, 2022* to create a new statutory framework governing personal information practices in the private sector. The bill is currently at second reading and will, if enacted, establish three new statutes:

- The *Consumer Privacy Protection Act* (CPPA), a private sector law that will repeal and replace the personal information protection framework in the *Personal Information Protection and Electronic Documents Act*.
- The *Personal Information and Data Protection Tribunal Act*, which will establish an administrative tribunal to review certain decisions made by the Privacy Commissioner of

Canada and impose penalties for contraventions of the CPPA.

- The *Artificial Intelligence and Data Act* (AIDA), which will create a risk-based approach to regulating trade and commerce in AI systems.

The *Consumer Privacy Protection Act*

The proposed privacy framework within Bill C-27 is substantially similar to the former Bill C-11, which died on the order paper in 2021 prior to the federal election. Once enacted, failure to comply with the CPPA could expose organizations to fines of up to the greater of $25 million and the amount corresponding to 5% of worldwide turnover for the preceding fiscal year. Organizations could also be exposed to administrative monetary penalties of up to the greater of $10 million and the amount corresponding to 3% of worldwide turnover for the preceding fiscal year.

Among other key features of the CPPA as currently drafted is a requirement for organizations to implement a privacy management program. The CPPA also reinforces consent (especially express consent) as the primary authority for organizations to process personal information. However, it also clarifies and creates new "exceptions to consent" authorities for the collection, use or disclosure of personal information. These exceptions apply to certain defined standard "business activities" and to support "legitimate interests," subject to conditions.

The CPPA includes numerous provisions relating to the lawful processing of "de-identified" data and "anonymized" data. The proposed provisions clarify that anonymized information is outside the scope of the CPPA. The draft legislation also creates a special status for personal information of minors.

In certain circumstances – namely, where there could be a "significant impact" on the individual – the CPPA would provide individuals the right to request that businesses explain how a prediction, recommendation or decision was made by an automated decision-making system and how the information was obtained. Furthermore, individuals could request that the organization dispose of their personal information and the organization must comply in specific circumstances.

Finally, the CPPA includes provisions granting individuals data mobility rights, allowing them to direct the transfer of their personal information from one organization to another.

The *Artificial Intelligence and Data Act*

In addition to establishing a new privacy legislative framework, Bill C-27 would enact AIDA, the first law in Canada regulating the creation and use of artificial intelligence systems. If enacted, AIDA would create a significant penalty regime, including fines for contravention of up to 3% of global revenue or C$10 million and fines of up to 5% of global revenue or C$25 million for more serious offences – or imprisonment, in the case of an individual.

Key elements of the proposed framework for regulating AI systems include mandatory assessments to determine whether an artificial intelligence system is a high-impact system, a term to be defined in the regulations. Organizations must publish a description and explanation of each high-impact system and must mitigate the risks of harm or biased output from use of such system.

AIDA also creates both self-reporting requirements for organizations and ministerial powers to order production of records, conduct an audit, publish warnings and order the

cessation of use or distribution of a high-impact system. AIDA further contemplates the appointment of an Artificial Intelligence and Data Commissioner to assist in the administration and enforcement of the legislation.

Bill C-26

Also in June, the Government of Canada introduced Bill C-26, *An Act Respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, for its first reading in Parliament. The bill seeks to create new powers for the federal government to respond swiftly and with agility to national security threats affecting federal critical infrastructure systems.

Bill C-26 would enact the *Critical Cyber Systems Protection Act* (CCSPA) to "provide a framework for the protection of the critical cyber systems of services and systems that are vital to national security or public safety." Critically, the CCSPA provides for administrative monetary penalties of up to $15,000,000 for each violation.

Specifically, the CCSPA would allow Cabinet to designate any service or system as "vital," a list that presently includes telecommunications services, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems within federal legislative authority, banking systems, and clearing and settlement systems. "Designated operators" in respect of a vital service or system would be required to establish a cybersecurity program.

The CCSPA would also impose obligations on designated operators to immediately report cybersecurity incidents to the Communications Security Establishment, as well as to one of several applicable regulatory authorities. Designated operators would also be required to maintain cybersecurity records.

The CCSPA grants powers to designated regulatory authorities, which include the Office of the Superintendent of Financial Institutions, the Minister of Industry, the Bank of Canada, the Canadian Nuclear Safety Commission, the Canadian Energy Regulator and the Minister of Transport, to ensure that designated operators comply with the CCSPA. These powers include the authority to enter places and the power to order internal audits, as well as the power to issue compliance orders and enter into compliance agreements.

Bill C-26 would also amend the *Telecommunications Act*, creating a new executive power to direct telecommunications service providers to do anything, or refrain from doing anything, that is necessary to secure the Canadian telecommunications system. Associated regulations and orders would be backed by an administrative monetary penalty scheme contemplating fines of up to $15 million for non-compliance.

Other provinces: A slower pace of change

Although it is widely expected that other provinces will follow Québec's lead in reforming (or creating) provincial private sector privacy legislation, the pace of change is much slower than in Québec or federally. Here is a snapshot update of legislative reform progress in British Columbia, Alberta and Ontario.

British Columbia

In February 2020, the British Columbia Legislative Assembly struck a special committee to

review the provincial *Personal Information Protection Act*. The special committee's recommendations [PDF] include creating stronger enforcement powers for the regulatory authority, such as the power to levy penalties. Also recommended is the creation of security breach notification requirements and data portability rights, as well as the establishment of pseudonymized data and sensitive information as new classes of data. The recommendations further contemplate the creation of specific employee privacy and health privacy regimes.

At present, the Government of British Columbia has not yet introduced a bill seeking to implement any of these proposed reforms.

Alberta

The Ministry of Service Alberta solicited feedback on privacy legislative reform in the summer of 2021 and conducted targeted focus groups in the fall of that year. However, the Province has not yet introduced a bill reforming the *Personal Information Protection Act* [PDF].

Ontario

The Government of Ontario initiated a consultation regarding the development of a comprehensive private sector privacy law in 2020 and published a white paper on the subject in 2021. However, there has been no further progress towards legislative reform following the provincial election in June 2022.

In addition, the Government of Ontario introduced a new transparency requirement in April 2022, when the provincial *Employment Standards Act* was amended to provide that Ontario-based organizations with more than 25 employees must implement an electronic employee monitoring policy. The Information and Privacy Commissioner of Ontario has stated that, while these amendments are a good first step to help Ontarians understand their employers' practices, workplace electronic monitoring should be governed by comprehensive provincial private sector privacy legislation. Additional information regarding the electronic monitoring policies is included in our Labour and Employment article.

What to expect in 2023

Continued major changes to the Canadian federal and provincial privacy landscape are likely forthcoming next year. Given the significant compliance costs and the threat of severe monetary fines in the future (most imminently in Québec), we encourage all companies to proactively consider the new and pending changes and to plan for their implementation.