NOVEMBER 20, 2020

New Privacy Law for Canada: Government Tables the *Digital Charter Implementation Act, 2020*

Authors: Elisa K. Kearney, Alysha Manji-Knight, Teraleigh Stevenson and Gillian R. Stacey

With dramatic growth in the global data economy, and increased reliance on online activity as a result of the global pandemic, protection of privacy and personal information has never been as relevant as it is now. Like many other jurisdictions, Canada has recognized the need for a significant revamp of its privacy laws to address challenges relating to increased international data flows.

After years of consultations, proposals and reports on Canada's privacy regime, the federal government tabled Bill C-11, the *Digital Charter Implementation Act, 2020,* on November 17, 2020. Bill C-11 significantly overhauls Canada's federal privacy laws and if adopted would (i) repeal Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the Act that currently governs the treatment of personal information and privacy; (ii) introduce the *Consumer Privacy Protection Act* (CPPA), which would govern privacy in the private sector; and (iii) introduce a new Personal Information and Data Protection Tribunal (Tribunal) governed by the new *Personal Information and Data Protection Tribunal Act*. The surviving Part 2 of PIPEDA, which relates to electronic documents, would be recast as the *Electronic Documents Act*.

Bill C-11 results from an extensive process of study and consultation. After the last formal review and amendment to PIPEDA in 2015 and a comprehensive review of PIPEDA released by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) in 2018, the government launched a national consultation on digital transformation and expressed its commitment to reforming the existing privacy regime. In the ensuing years, several reports and proposals have been produced by ETHI, the Office of the Privacy Commissioner and the Ministry of Innovation, Science and Economic Development. In 2019, the government introduced its Digital Charter, which was intended to provide a principled framework for the development of privacy laws across Canadian jurisdictions. Throughout this process, the federal government has emphasized the importance of balancing, on the one hand, the protection of privacy as a fundamental value and, on the other hand, the important role of personal information in business, trade and commerce in a modern, data-driven global economy.

Important Changes

Although Bill C-11 maintains a principles-based approach to privacy, and not the rights-based legislation the federal Privacy Commissioner favoured, there is a renewed emphasis on the role of transparency, accountability and consent as governing principles of Canada's privacy regime, which is evident in some of the most notable provisions of Bill C-11:

- **Significant Administrative Monetary Penalties (AMPs).** The CPPA would significantly expand the penalties available for contravention of federal private sector privacy law. AMPs of up to $25 million or 5% of an organization's gross global annual revenue, whichever is greater, could be imposed for contravention of the CPPA. More specifically, the CPPA proposes an AMP of $10 million or 3% of an organization's gross global annual revenue for contravention of provisions relating to consent, collection, use, retention and disposal of personal information and certain security safeguard provisions. For more egregious conduct, the CPPA would impose AMPs of $20 million or 4% of an organization's gross global annual revenue for offences punishable by summary conviction and $25 million or 5% of an organization's gross global annual revenue for indictable offences. In particular, such AMPs are available when an organization knowingly contravenes provisions relating to reporting of security safeguard breaches, maintaining records of safeguard breaches, retaining information subject to an access request, using de-identified information to identify an individual, denying whistleblower protections or obstructing an investigation, inquiry or audit of the Privacy Commissioner.

- **Private Right of Action.** A new private right of action against organizations for damages for loss or injury would be available to individuals. In particular, when the Privacy Commissioner finds that an organization has contravened the CPPA and either such organization does not appeal the decision to the Tribunal or the Tribunal dismisses the appeal, or when the Tribunal determines that an organization has contravened the CPPA, individuals affected by the organization's conduct could seek damages in either Federal Court or a provincial superior court for loss or injury suffered as a result of the organization's conduct.
- **Expanded Privacy Rights.** The CPPA would introduce new rights that would provide individuals with greater control over their data and how they are used, including the following:
    i. *Data portability.* An individual may request that an organization transfer the individual's personal information to another organization;
    ii. *Erasure*. An individual may request that an organization dispose of all personal information that the organization has collected from the individual; and
    iii. *Explanation*. An individual may request that an organization explain the predictions, recommendations or decisions made about that individual using automated decision systems.
- **Automated Decision-Making Transparency.** The CPPA would require organizations to disclose *any* use of automated decision systems to make predictions, recommendations or decisions about individuals that could have a significant impact on such individuals.
- **Modernized Consent Requirements**. Consistent with the approach under PIPEDA, the CPPA would maintain consent as the primary grounds to justify collection, use and disclosure of personal information. Meaningful consent under the proposed legislation would require that certain disclosures be provided in simple and plain language. Only if such requirements are adhered to would consent be valid. Moreover, while PIPEDA requires express consent only for particularly sensitive information, express consent would be the default under the CPPA. Finally, the CPPA would expand the list of exceptions to the requirement of consent to include a range of business activities, transfers to service providers, de-identification, research and development, prospective and completed business transactions, employment information and certain public interest exceptions.
- **De-identification Rules.** The draft legislation contains provisions on the de-identification of personal information. Organizations would be required to ensure that the technical and administrative measures applied to de-identified information are proportionate to the purpose of the de-identification and the sensitivity of the information. As noted above, misuse of de-identified information would be punishable by more severe AMPs. Under the CPPA, organizations would be prohibited from any use of de-identified information to identify an individual, except to test the effectiveness of security safeguards. Organizations would be permitted to de-identify personal information without the individual's knowledge or consent.
- **New Powers of the Privacy Commissioner.** Under the CPPA, the Privacy Commissioner would have broad order-making powers to mandate compliance with the CPPA and prohibit organizations from collecting or using personal information under certain circumstances, as well as the power to audit the personal information management practices of an organization when the Privacy Commissioner has reasonable grounds to believe that the organization has contravened the CPPA. Separately, the Privacy Commissioner would be permitted to make recommendations on AMPs to the Tribunal. Finally, the Privacy Commissioner would have the ability to approve codes of practice and certification systems voluntarily submitted by private organizations. If approved, the code/certification system would effectively establish the legal obligations of the organization.
- **Personal Information and Data Protection Tribunal.** The Tribunal would have jurisdiction over the Privacy Commissioner's orders and any appeals of the Privacy Commissioner's findings on contraventions of the CPPA. The Tribunal would also have final say on whether AMPs should be levied against a company and the amount of such penalties.

- **Separating Privacy and Electronic Documents.** As noted above, if the legislation is passed, it would repeal Part 1 of PIPEDA and change the name of the surviving legislation to the *Electronic Documents Act*. As the new short title suggests, this Act would be largely limited to electronic documents, while the new CPPA would govern personal information and privacy in the private sector.

The bill may not have smooth sailing through the legislative process. For example, the shift to what is overtly a consumer protection framework could spur constitutional challenges because consumer protection laws typically fall within provincial and territorial jurisdiction. In his statement on Bill C-11, the Privacy Commissioner also alluded to potential constitutionality issues of Bill C-11, noting that "only the provinces have jurisdiction to legislate civil rights matters and the federal Parliament's jurisdiction is limited to trade and commerce." However, the Privacy Commissioner also referred to the Supreme Court of Canada's recent finding that "privacy is of vital interest" and is "validly subject to protection in several federal statutes made under one or another of the heads of power Parliament" and "should also apply to the [CPPA], enacted under the trade and commerce powers of Parliament." The Privacy Commissioner also commented that "the Bill raises a number of questions about its ability to effectively protect privacy in a constantly evolving digital society." But whether all or only some of the proposed changes come to pass, businesses will likely have a higher compliance burden.

We will continue to closely monitor the debate around Bill C-11 and update our clients on what steps they can take to ensure that if Bill C-11 is enacted, they are in a position to quickly implement changes to their privacy management practices, ensuring that they remain onside of Canada's privacy laws.

Read the full text of Bill C-11.

Key Contacts: Elisa K. Kearney and Elliot A. Greenstone