

Preliminary Overview of New Federal Privacy Bill

June 16, 2022

Introduction

This document outlines key elements of Bill C-27 – new legislation tabled by the federal government on June 16, 2022.

Bill C-27, If passed, would replace PIPEDA – Canada’s current privacy law for the private sector – with a new law, to be known as the *Consumer Privacy Protection Act (COPA)*.

In addition, the bill introduces proposals to regulate the use of artificial intelligence (AI) through the *Artificial Intelligence and Data Act*. The CMA will provide a separate brief on the AI components of the bill at a later time.

If you wish to review the full text of Bill C-27, click [here](#).

The CMA [issued a statement](#) welcoming the bill, and noting the urgent need for balanced, modernized privacy law. We will be actively involved in consultations with government and conversations with parliamentarians to support further study of the bill.

It is important for marketers to note that for the foreseeable future, PIPEDA will remain in effect. Before any bill becomes law, it goes through an extensive review process in the House of Commons and the Senate and provisions could change. Once a bill is adopted, the government determines the date on which it will come into force. The government has acknowledged that organizations will require a significant transition period to adapt their processes and train staff to adhere to the new law.

Be sure to subscribe to our weekly Top 5 Picks newsletter for key updates.

Major Privacy-Related Provisions for Marketers

This is not an exhaustive list of obligations for organizations. Rather, it focusses on provisions in the bill of particular importance to the marketing sector – some which differ from PIPEDA – to help marketers prepare for meaningful conversations with their compliance teams.

[CMA members can click here](#) to review a more detailed description of Bill C-27, including a comparison to the provisions of Bill C-11, which was introduced in 2020 but not adopted prior to the election.

Overall context

- The bill is principles-based and technologically neutral – an approach that the CMA and other industry groups strongly advocated for.
- The bill has a balanced purpose statement, recognizing both privacy protection and commercial interests. It notes the need for Canadians to benefit from the digital and data-driven economy, and from essential international data flows.
- The right to privacy is acknowledged but appropriately, is not referred to as a “fundamental human right”.

Who the Act would apply to

- The Act would apply to organizations, regardless of whether personal information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization.
- If a service provider collects, uses or discloses personal information for any purpose other than the purposes for which the information was transferred, it would be subject to the Act.
- Transfers of personal information to service providers for processing would continue to be permitted without requiring new knowledge or consent from customers.

Consent

- The Act proposes to preserve Canada's model of express/implied consent, but with some changes.
- Express consent would be required for the collection, use, and disclosure of personal information unless the organization establishes that it is appropriate to rely on an individual's implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the personal information.
- For consent to be valid, an organization would be required to provide the individual (e.g., in their privacy policy) with a prescribed list of information outlined in the Act, in plain language.
- The bill proposes new exceptions to consent for the collection and use of personal information, including for a prescribed list of business activities, and for when the organization has a legitimate interest that outweighs any potential adverse effect on the individual. To rely on legitimate interests, an assessment needs to be made by the organization that could be subject to inspection by the regulator.
- An organization would be permitted to use an individual's personal information without their knowledge or consent to de-identify the information, and could use de-identified information for internal research, analysis and development purposes.

Children's data

- The personal information of minors would be considered to be sensitive information.
- Parents or guardians could exercise the Act's rights and recourses on behalf of their child.

Openness and transparency requirements

- The Act includes enhanced general transparency requirements for organizations, including to provide an account of an organization's use of automated decision systems to make predictions, recommendations or decisions about individuals (but only those that could have a significant impact on them), and information on the retention periods applicable to sensitive personal information.
- Under certain circumstances, organizations would have to make certain information available at an individual's request, including the names of third parties or types of third parties to which they disclose their information, and an explanation of any prediction, recommendation or decision made about a person using an automated decision system (but again, only those that could have a significant impact on them).

Disposal and retention of data

- An organization would not be able to retain personal information for a period longer than necessary to a) fulfill the purposes for which the information was collected, used or disclosed or b) comply with the requirements of the Act, of federal or provincial law or of the reasonable terms of a contract.
- If an organization receives a written request from an individual to dispose of their personal information, it would be required to do so as soon as feasible. However, the obligation is subject to a number of practical exceptions, including if the information is not in relation to a minor, it is scheduled to be disposed of in accordance with the organization's information retention policy,

and the organization informs the individual of the remaining period of time for which the information will be retained.

Data mobility

- Individuals would have the right to direct the transfer of their personal information from one organization to another, if both organizations are subject to a data mobility framework provided under the regulations.

De-identified and anonymized Information

- The Act distinguishes between anonymization and de-identification:
 - To anonymize would mean to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual could be identified from the information, whether directly or indirectly, by any means. It could be used as a way to dispose of information.
 - To de-identify would mean to modify personal information so that an individual could not be directly identified from it, though a risk of the individual being identified would remain.
- De-identified information would be considered personal information subject to the Act. However, some sections of the Act would not apply, including some situations where consent was not required.
- There would be a requirement to protect de-identified information with technical and administrative measures proportionate to the purpose and sensitivity.
- An organization would not be permitted to use information that had been de-identified, alone or in combination with other information, to identify an individual, except under certain exceptions, including if the Privacy Commissioner permitted it.