Cassels

Repackaging PIPEDA for a GDPR World

Bernice Karn

November 19, 2020

Since 2018 the European Union has set the global standard for privacy regulation through the enactment of the *General Data Protection Regulation* (GDPR), and since then it has been Canada's turn to play catch-up. To that end, Canada has finally taken a major step toward modernizing its private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) though the introduction of the Bill C-11, the *Digital Charter Implementation Act, 2020* in the House of Commons on November 17, 2020. If enacted, Bill C-11 would significantly amend PIPEDA to create the *Consumer Privacy Protection Act* (CPPA), the *Personal Information and Data Protection Tribunal Act* (PIDPTA), and usher in a new era of privacy regulation in Canada that is comparable to the GDPR and the *California Consumer Privacy Act*. Businesses that contravene Canada's privacy laws could face penalties of up to $10 million or 3% of global revenues and class actions for damages under this legislation.

The three pillars of Bill C-11 are: enhancing individuals' control over their personal information, encouraging responsible innovation, and improving privacy oversight and enforcement. In furtherance of those principles, the new legislation seeks to do the following:

- increase transparency around how organizations handle personal information,
- give individuals more control over how their personal information is handled,
- require that requests for consent and privacy policies be expressed in clear and plain language, and
- provide the Office of the Privacy Commissioner of Canada (OPC) with the power to make orders, conduct inquiries and recommend significant administrative monetary penalties to the newly established Personal Information and Data Protection Tribunal. **Click here to read more about the new penalties and enforcement powers**.

What Does the New Privacy Legislation Mean for Canadian Organizations?

Although PIPEDA has governed private sector organizations in Canada for almost two decades, should Bill C-11 become law, those organizations will have to review their privacy practices and policies and update them to ensure that they are compliance with the new regime. This will mean more than just re-reading and changing a few words in a privacy policy. Organizations will have to take a careful look at how and why they collect, use and disclose personal information, determine if those purposes are objectively reasonable, develop new written policies and procedures to accurately reflect those practices – and then follow them.

Organizations should pay particular attention to the following significant compliance aspects:

1. **Mandatory Privacy Management Programs.** Under PIPEDA organizations are required to be open about their policies and practices with respect to their management of personal information and only certain limited information is required to be disclosed about those policies and practices. For many organizations this “openness” typically takes the form of simply having a privacy policy, sometimes with little regard to following its actual provisions in practice. Under Bill C-11, the requirement is expanded for organizations to go beyond a privacy policy and have a “privacy management program.”

Under a privacy management program, the organization must have policies, practices and procedures for: the protection of personal information; dealing with requests for information and complaints; training for staff and information to be provided to staff about the policies, practices and procedures; and “development of materials” to explain the organization’s policies and procedures. The “development of materials” language suggests that more than a privacy policy is required – perhaps videos and interactive digital media might be in order.

The volume and sensitivity of the personal information held by an organization are to be considered in its development of a privacy management program, which suggests that an organization handling large volumes of personal information and sensitive information must put into place a program that is more robust than the programs to be implemented by other organizations that handle relatively little personal information that is not particularly sensitive.

Policies must be openly available, transparent, written in plain language, and they must disclose, among other things, the use of any automated decision-making systems and whether the organization transfers personal information internationally or interprovincially.

2. **Consent**. PIPEDA is based on the concept of obtaining some form of informed consent, whether express, opt-out or implied, to the collection, use or disclosure of personal information. However, now Bill C-11 has raised the bar and the new default rule will be express consent. The onus will be on the organization to establish that it is appropriate for the organization to rely on implied consent, given the reasonable expectations of the individual and the sensitivity of the information. Therefore, it is likely that an organization may only rely on implied consent if its personal information processing activity is within the individual's reasonable expectations and the information is of low sensitivity.

Bill C-11 mandates specific requirements for the disclosure that must be given in a request for consent, in plain language. These requirements include: a statement of the purposes for the collection, use and disclosure of personal information; a description of how personal information will be collected, used and disclosed; the foreseeable consequences of the collection, use or disclosure; a list of specific types of information to be collected, used and disclosed; and the names of any third parties or types of third parties

to whom disclosure could be made.

Tempering this broad requirement for express consent is a new concept of “business activity,” which no doubt borrows from the “legitimate interest” approach in the GDPR and provides some measure of flexibility for organizations to collect and use personal information in their day-to-day operations without consent. Note that the exception refers only to collection and use, not disclosure. Consent is not required to collect or use personal information for a “business activity” where a reasonable person would expect collection or use for that activity and the personal information is not collected or used to influence the individual’s behaviour or decisions. The following six categories are listed as business activities in Bill C-11:

(a) an activity that is necessary to provide or deliver a product or service that the individual has requested from the organization;

(b) an activity that is carried out in the exercise of due diligence to prevent or reduce the organization’s commercial risk;

(c) an activity that is necessary for the organization’s information, system or network security;

(d) an activity that is necessary for the safety of a product or service that the organization provides or delivers;

(e) an activity in the course of which obtaining the individual’s consent would be impracticable because the organization does not have a direct relationship with the individual; and

(f) any other prescribed activity.

These business activities are expressed in fairly broad terms and could be liberally interpreted by organizations seeking to avoid obtaining consent. However, given the severities of potential penalties under this bill, pushing the envelope on consent might carry harsh penalties. Businesses will need clear guidance from the OPC and ultimately the courts on the scope of these exceptions. It is anticipated that organizations will have to document their analysis and reasons for their reliance on this business activity exception as part of their privacy management programs.

3. **Enhanced Individual Control over Personal Information.** PIPEDA provides individuals with a right of access to the personal information that organizations hold about them, subject to some limited exceptions. It also gives individuals a right to correct or supplement information that they can demonstrate is incorrect or incomplete. Bill C-11 adds to these rights by giving individuals a data portability right to have their information moved from one organization to another, provided that both organizations are part of a “data mobility framework” that is to be set out in future regulations. By way of example, this data mobility framework could set the technical parameters for the transfer of

personal information between social media platforms or banking platforms.

PIPEDA is ambiguous about whether individuals have the right to require that the organization delete their personal information. Bill C-11 dispels any ambiguity about this issue by giving individuals the right to require that organizations "dispose" of their personal information, unless: (i) the disposal would result in the disposal of personal information of another individual and that other information cannot be severed, or (ii) the CPPA, another Canadian federal or provincial law, or the "reasonable terms" of a contract prevent such disposal. Note that "disposal" means "permanent and irreversible deletion". We can expect disputes to arise over the meaning of "reasonable terms" of a contract. While there is no explicit "right to be forgotten" in Bill C-11, it seems likely that this deletion right will be the tool that individuals use to accomplish that goal.

4. **Outsourcing and Service Providers.** In 2019 the topic of outsourcing and transborder data flows was of considerable interest to the OPC. Readers may recall that the OPC proposed a potential requirement for organizations to obtain individuals' consent to the outsourcing of their personal information to service providers and conducted a consultation to that effect. (See our previous articles (on April 16, 2019; June 12, 2019; and September 24, 2019.) Ultimately the OPC took the view that consent was not required, and that stance has been memorialized in Bill C-11, which will be of relief to many in the business community. Bill C-11 has also clarified that, should a service provider determine that a security breach has occurred involving personal information, the service provider has an obligation to report such breach to the organization that provided such information, rather than to the OPC directly.

Part of the OPC's 2019 consultation considered cross-border transfers of personal information in the outsourcing context. Interestingly, Bill C-11 is silent on any restrictions on cross-border data flows, except for the requirement to include information about the potential for such transfers in readily available, plain language privacy policies and only if the transfer or disclosure "may have reasonably foreseeable privacy implications." This largely codifies existing custom in Canada, based on OPC guidance, to provide notification to individuals of cross border transfers/disclosures and the potential access by law enforcement in other jurisdictions.

5. **Automated Decision Systems.** A new feature to Canadian privacy law that Bill C-11 introduces is the concept of automated decision systems, which are defined as:

"any technology that assists or replaces the judgement of human decisionmakers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets."

Bill C-11 would obligate organizations to provide a general account of their use of these automated decision systems to make predictions, recommendations or decisions about individuals that could have a significant impact on those persons. In addition, upon request of the individual, organizations must provide an

explanation of the prediction, recommendation or decision made about the individual and how the individual's personal information was used in the process to arrive at the result. This does not amount to publication of decision-making algorithms per se, but requires clear, plain language descriptions of the ways in which they work. Unlike the GDPR, Bill C-11 does not include a right to object that is specific to automated decision systems.

6. **De-identification of Personal Information.** Many organizations today deal with “anonymized” or “de-identified data” that are derived from personal information, and it is often a point of contention as to whether the organization actually has the right to use the personal information for that purpose – i.e., to process and render it into anonymized or de-identified form. Bill C-11 clears up the use issue by explicitly permitting the de-identification of personal information without knowledge or consent. However, it also requires that any administrative or technical mechanisms applied to personal information that is to be de-identified are proportionate to the purpose for which de-identification is being undertaken and the sensitivity of personal information.

Interestingly, in the case of a prospective business transaction where PIPEDA has laid out a framework that the parties to the transaction can follow to disclose and use personal information for the purposes of due diligence and completing the transaction, Bill C-11 adds a twist. Under this proposed law, the framework would also require that the personal information be de-identified before it is used and disclosed, and it must remain de-identified until the transaction is completed. The practicality of such a provision remains to be seen, especially in transactions involving key individuals where it may be critical to know their identities.

Re-identification of individuals through the use of de-identified information is a concern and becomes increasingly important as new technologies make re-identification a reality. Fortunately, Bill C-11 addresses this by prohibiting the use of de-identified information, alone or in combination with other information, to identify an individual except to test the security safeguards used to protect the information.

What Isn’t in Bill C-11?

While this proposed legislation is a step towards a more robust privacy regime in Canada, it has not gone as far as the GDPR. For example, besides the lack of specific prohibitions on cross-border data transfers and no explicit “right to be forgotten” as discussed above, Bill C-11 does not mirror the “controller”/“processor” structure of the GDPR, it does not mandate any type of registration process with the OPC, nor does it contain granular technical data protection requirements that one sees in the data protection laws of some jurisdictions. This bill strikes a middle ground between our existing privacy regime under PIPEDA and the more complex world of the GDPR.

Next Steps

As at the writing of this article, Bill C-11 has just been introduced in the House of Commons and is at the first reading stage. Second reading and referral to committee for further review and study will follow. However, given that there presently is a minority government in Parliament, the future of this bill is unclear. We will continue to monitor the bill as it proceeds through Parliament and will keep our readers updated on further developments.
