Bill C-11: A Closer Look (Part 1 of 2)

Proposed Acts and Proposed Changes to Individual Rights

Fraser Mann and Anna Troshchynsky December 9, 2020

Bill C-11, the *Digital Charter Implementation Act, 2020* (the "Bill") was introduced on November 17, 2020 by Canada's Innovation, Science and Industry Minister, Navdeep Bains, in the House of Commons. The Bill is a first major overhaul of Canada's federal privacy legislation in the past 20 years, since the enactment of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). The Bill proposes substantial changes to modernize the current privacy laws dealing with the protection of personal information collected, used and disclosed by private sector organizations in Canada.

This is Part 1 of a two-part commentary that summarizes the major changes introduced by the Bill in relation to PIPEDA:

> **Part 1** discusses the Bill and the proposed amendments to the consent requirements, uses of de-identified information, algorithmic transparency and other enhanced individual rights.
>
> **Part 2** provides an overview of the proposed requirements on organizations, the enforcement regime and penalties.

For discussion purposes, reference will be made to the existing federal privacy regime, Ontario's *Personal Health Information Protection Act* ("PHIPA"), Quebec's proposed Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (the "Quebec Bill") and the *European Union's General Data Protection Regulation* ("GDPR").

Note that the information presented here is based upon the first reading of the Bill tabled in the House of Commons on November 17, 2020 and is subject to change, as the Bill may be amended as it goes through the legislative process before becoming law

New Proposed Legislation

The Bill introduces: (i) the *Consumer Privacy Protection Act* (the "CPPA"), which repeals Part 1 of PIPEDA dealing with protection of personal information by private sector organizations and other organizations that collect, use or disclose personal information in the course of commercial activities; and (ii) the *Personal Information and Data Protection Tribunal Act* (the "PIDPTA") which establishes the Personal Information and Data Protection Tribunal (the "Tribunal") to impose penalties and hear appeals under the CPPA.

Consent Requirements

Informed Consent

The CPPA addresses requirements relating to consent. Organizations must obtain valid express consent from individuals before or at the time of collection and provide them with information in *plain language* about (section 15 of the CPPA):

(i) the purpose of the collection, use or disclosure of their personal information;

(ii) the way in which their personal information will be handled;

(iii) any foreseeable consequences to such collection, use or disclosure; and

(iv) the ways in which organizations may share personal information with third parties.

Organizations will be able to rely on implied consent in certain circumstances, subject to an individual's reasonable expectations and the sensitivity of the personal information. With the exception of informing individuals of foreseeable consequences, much of this will not be new to any organization that has aligned its privacy and data-handling practices with best practices and guidance issued by the various privacy commissioners over the past twenty years (for example Schedule 1 of PIPEDA and the Office of the Privacy Commissioner of Canada ("OPC") guidelines for obtaining meaningful consent).

Informing individuals of the foreseeable consequences to a collection, use or disclosure may prove challenging.

It is not immediately apparent how or where to draw the line on what is or is not foreseeable.

Implied Consent for Business Activities

The transfer of personal information without an individual's knowledge or consent is permitted for certain purposes related to business activities, such as:

(i) an activity that is necessary to deliver a product or service;

(ii) an activity carried out in the exercise of due diligence to prevent or reduce the organization's information, system or network security;

(iii) an activity necessary for the safety of a product or service; or

(iv) other circumstances in which obtaining the individual's consent would not be practicable.

In all such cases, however, it must be shown that a reasonable person would expect the collection or use of the personal information for the specified purposes, and the personal information must not be collected or used for the purposes of influencing the individual's behaviour or decisions (section 18 of the CPPA).

While PIPEDA provides for implied consent, section 18 of the CPPA is more detailed, and the prohibition on influencing an individual's behaviour or decisions is noteworthy. Will targeted advertising on a free online service be a violation? Will the use of demographic or other personal information to determine what news stories someone views be a violation? Some current practices may run afoul of this provision.

Implied Consent for Transfers to Other Organizations

Consent is not required for the transfer of personal information to an organization's service provider (section 19 of the CPPA).

In addition, consent is not required for use and disclosure between organizations that are parties to a prospective business transaction if the information is *de-identified* before use and disclosure and remains so until the transaction is closed, subject to certain requirements relating to use of the information by appropriate security safeguards (section 22 of the CPPA). Upon closure of the transaction, the information may be disclosed and used in identified form, subject to the parties

having entered into an agreement:

(i) permitting use of the information only for the purposes for which it was originally collected;

(ii) protection of the information by appropriate security safeguards;

(iii) continuing compliance by both organizations with the terms of the agreement; and

(iv) notification to affected individuals that their information has been disclosed as part of the business transaction.

However, organizations engaging in a business transaction cannot rely on implied consent if the primary purpose or result of such transaction is the purchase or other dealing with personal information.

Having clear rules that address the disclosure of personal information in the context of mergers and acquisitions will help to avoid some of the difficulties that arise when a target organization's privacy policy does not expressly allow for this type of disclosure.

Changes to Consent in General

In general, incorporating the explicit consent requirements in the CPPA will codify the overarching consent principles in the guidelines provided by the OPC to promote transparency and simplify organizations' privacy policies such that Canadians better understand how their information is collected and used.

Uses of De-identified Information

De-identified Information in General

The CPPA proposes new rules around the use and protection of *de-identified* information that are not present under PIPEDA. Under the CPPA, to de-identify information means to "modify personal information — or create information from personal information — by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual".

Specifically, an organization:

(i) may use individual's personal information without their knowledge or consent to de-identify the information, which may in turn be used for internal research and development purposes (sections 20-21 of the CPPA);

(ii) cannot use de-identified information or combine it with other information to identify an individual (section 75 of the CPPA); and

(iii) must ensure that any technical and administrative measures applied to de-identified information are proportionate to the sensitivity of the information and the purpose for which it is de-identified (section 74 of the CPPA).

Organizations can face substantial penalties for knowingly identifying individuals using de-identified data, except in certain circumstances (penalties will be discussed in detail in Part 2 of this commentary). The Quebec Bill proposes an analogous exception to the use of de-identified

information for internal study or research purposes (section 102 of the Quebec Bill).

These new changes in the CPPA will have implications for agreements made for the provision of services, especially services that host or process personal information or where the use of the services results in the collection of personal information.

For example, consider a service agreement for a cloud-based service. Most include a provision that permits the service provider to monitor use, aggregate use information across its customer base, and use that information for purposes of providing services and improving its products and services. The proposed changes would allow use of de-identified information for these purposes even in the absence of a provision setting out this right in the agreement. Still, some service providers include provisions in their standard agreement that give them much broader use rights in relation to aggregated data.

This raises an interesting question: will the introduction of statutory penalties for failing to properly de-identify aggregated personal information cause service providers to step back from these more aggressive provisions?

Use of De-identified Information for a Socially Beneficial Purpose

The CPPA introduces a new "socially beneficial purpose" exception where organizations will be permitted to disclose *de-identified* information without individuals' knowledge or consent. Specifically, organizations may disclose *de-identified* information to a government institution, health care institution or any other organization mandated to carry out a socially beneficial purposes related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose (section 39 of the CPPA).

This provision should prove helpful to organizations engaged in research and study in connection with the development of vaccines or new modes of treatment for infectious diseases such as COVID-19. There are questions, however, as to the scope of what could be considered as socially beneficial.

It will be interesting to see if the regulations made under the CPPA provide further guidance on:

(i) what is a "socially beneficial purpose";

(ii) who may decide what is and what is not a socially beneficial purpose; and

(iii) how an honest misjudgment when deciding whether or not a purpose is "socially beneficial" will be handled.

Right to Algorithmic Transparency

The CPPA provides a new right for an individual to request that an organization provide an explanation about the automated decision system used to arrive at a prediction, recommendation or decision affecting them and how the personal information was used (section 63(3) of the CPPA).

The CPPA defines an automated decision system as "any technology that assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets".

As part of the openness and transparency requirements, an organization must also provide a "general account" of its use of any automated decision system that could have significant impacts on individuals within the organization's policies and practices (section 62(2)(c) of the CPPA).

Notably, the Quebec Bill specifically mandates an organization to inform concerned individuals at the time or before a decision based exclusively on automated processing is made about them, in addition to providing the reasons and principal factors that led to the decision upon request (section 102 of the Quebec Bill).

PIPEDA already has provisions requiring organizations to keep personal information used to make a decision about an individual for a period of time after the decision is made to enable individuals to understand how the decision was made. Making it possible for individuals to review and challenge the decisions made by human actors is an important right in PIPEDA.

With increasing numbers of decisions being made by algorithms, this right could be eroded, especially if the creators of the algorithms refuse to disclose how the algorithms make decisions. The new right in the CPPA will require organizations to explain the working of the algorithm, on the basis of which any decision is made, reducing the erosion of the existing right and expanding its application to include both human and non-human decision making systems.

Right to Data Mobility

The CPPA affords individuals a new right to request that an organization disclose (or "port"), the personal information it collected about them to another designated organization, provided that both such organizations are subject to a data mobility framework to be specified in future regulations (section 72 of the CCPA).

The CPPA does not include much more detail, except that such regulations may specify the organizations subject to the data mobility framework, the applicable exceptions to the disclosure requirement and the security safeguards that should be put in place to facilitate such data transfers (section 120 of the CCPA). Nonetheless, the introduction of this new right marks a significant change that is set to increase an individual's control over his or her personal information and will require organizations to put procedures and processes in place to comply with these requests once the regulations are settled.

Right to Disposal

The CPPA creates a new right for an individual to request an organization to dispose of (i.e. permanently delete) their personal information that the organization has collected (section 55 of the CPPA). An organization may refuse an individual's request only where it would result in disposing of personal information about another individual, or where federal, provincial or reasonable contractual requirements would prevent the organization from doing so.

If an organization fulfills the individual's request and has transferred the personal information subject to the request to any of its service providers, it must also notify such service providers of the disposal request and confirm that they have also disposed of the information.

While this new right to disposal of personal information does not give individuals an explicit "right to be forgotten", it is nonetheless a step in that direction and appears to be inspired by the right to erasure under Article 17 of the GDPR.

Notably, the new right in the CPPA is less prescriptive compared to the changes proposed in Quebec. The Quebec Bill proposes to allow an individual to require an organization to "cease dissemination" of personal information about them or to "de-index any hyperlinks" providing access to that information when certain conditions are met (section 113 of Quebec Bill).

Other Enhanced Rights

The CPPA extends the rights under PIPEDA relating to access to personal information about an individual held by an organization. Subject to certain exceptions, an individual is entitled to:

(i) receive any information within 30 days of the request, and be advised of any extension of that time period (section 67 of the CPPA);

(ii) receive the information in an alternative format, if they have a sensory disability and request an alternative format (section 66 of the CPPA); and

(iii) be advised of any cost associated with responding to the request (section 68 of the CPPA).

An organization may deny access to personal information to an individual if that would likely reveal personal information about another individual (section 70 of the CPPA). If access is granted, an organization must retain information for the period necessary to enable an individual to exercise all rights available under the CPPA (section 69 of the CPPA).

As in the case of the present law, an organization must correct information that is not accurate, up-to-date, or complete. If appropriate, the amended information must also be transmitted to a third party (section 71 of the CPPA). The organization must record any disagreement with an individual about any amendments to be made to the information (and if appropriate, inform third parties about the disagreement).

Where an organization holds sensitive medical information about an individual, an organization may choose to give access to such information through a medical practitioner (section 66(3) of the CPPA). This provision is intriguing when read with provincial legislation dealing with the protection of personal health information.

For example, medical practitioners have a right not to disclose personal health information in circumstances where the disclosure may cause serious harm to the individual or to another person (section 52(e)(i) of PHIPA).

This is not quite the same as section 66(3) of the CPPA, which does not include a right to refuse to provide personal health information.

Alternatively, is section 66(3) intended to address the same circumstances as section 24(1)(2) of the *General Regulation* under PHIPA (O. Reg. 329/04)? That section exempts a laboratory from responding to requests about personal information in its custody or control if "the individual has a right of access to the information through the health care practitioner, or will have such a right when the information is provided by the laboratory to the health care practitioner within a reasonable time". If the intent of section 66(3) of the CPPA is the latter, it is less controversial.

Concluding Comments

The far-reaching proposed amendments to Canada's federal privacy laws will extend individuals'

rights to give their consent prior to the collection, use or disclosure of information about them held by an organization.

The new rights to algorithmic transparency and to data mobility are largely consistent with changes proposed in Quebec, as well as the GDPR.

The new compliance requirements and enforcement regime, discussed in Part 2 of this commentary, will give Canadians the confidence they need to enable them to protect the substantive rights granted under the new law.