Canada's Consumer Privacy Protection Act: Impact for businesses

On November 17, 2020, the Minister of Innovation, Science and Industry, Navdeep Bains, introduced Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, or *Digital Charter Implementation Act, 2020*. The proposal would modernize, and in certain respects toughen, Canadian private sector privacy law by enhancing transparency and control over personal information held by businesses, and imposing new, potentially onerous sanctions for non-compliance. This article focuses on the key differences between the federal government's current privacy framework, the *Personal Information Protection and Electronic Documents Act*, and its replacement, the *Consumer Privacy Protection Act*.

What you need to know

This article provides an overview of the key aspects of the CPPA and their impact on Canadian businesses. As more fully detailed herein, this new privacy regime would introduce the following changes:

- New enforcement tools:
    - The newly constituted Personal Information and Data Protection Tribunal would have powers to impose, upon recommendation by the Office of the Privacy Commissioner of Canada (Commissioner), administrative monetary penalties of C$10,000,000 or, if greater, the amount corresponding to 3 per cent of the organization's global gross revenues in its previous fiscal year.
    - Reinforced fines in the case of penal proceedings of a maximum of C$25,000,000, or, if greater, the amount corresponding to 5 per cent of the organization's global gross revenues in its previous fiscal year.
    - New private right of action for individuals.
    - New provisions to enable the creation of "codes of practice" and "certification programs".

- New individual rights inspired by European law: right to be informed of automated decision-making, right to disposal and right to mobility.

- Reinforced accountability rules:
    - New definition of the notion of "control".
    - New obligation to establish, implement and make available a privacy management program.
    - Clarity concerning the role and responsibilities of service providers.

- Reinforced consent requirements, including greater clarity concerning the notion of valid consent.

- Some less stringent rules: new consent exceptions for de-identified information, socially beneficial purposes and legitimate business practices.

Table of contents

Introduction

The federal government's proposal to modernize the *Personal Information Protection and Electronic Documents Act* (PIPEDA) – a legislation that was enacted nearly two decades ago, is as ambitious as it is cautious in its attempt to meaningfully enhance privacy protections for individuals. The proposal, which would effectively replace PIPEDA's privacy provisions with the *Consumer Privacy Protection Act* (CPPA), aims to operationalize the Canadian government's Digital Charter as well as past proposals to strengthen privacy in the digital age in order to address the challenges posed by the digital economy and new technologies. In addition, the proposal would enact the *Personal Information Data Protection Tribunal Act*, establishing a new Personal Information and Data Protection Tribunal (Tribunal), which would have the ability to impose significant penalties. Further, the most serious violations of the CPPA could result, upon prosecution, in fines, which have been described as the strongest among G7 privacy laws, including the European Union's General Data Protection Regulation (GDPR) and the *California Consumer Privacy Act of 2018* (CCPA).

While clearly inspired by similar initiatives in other countries, namely the EU's GDPR and California's CCPA, the Canadian proposal is unique in its approach in that, in many instances, it affords businesses with greater flexibility and clarity relative to the present privacy regime's requirements. Most notably, it borrows directly from past guidance and decisions issued by the federal privacy commissioner, the Office of the Privacy Commissioner of Canada (Commissioner), and provides individuals with new rights that are more narrowly framed than those currently found under the GDPR. In this sense, it bears noting that Québec Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* – a recent proposal that seeks to amendment Québec's provincial privacy regime, including the *Act respecting the protection of personal information in the private sector* – is considerably more onerous than the CPPA, raising a number of challenges from an interoperability standpoint for businesses operating at a national level. For a more detailed analysis of Québec Bill 64's proposed amendments, please see *Proposed amendments to Québec privacy law: Impact for businesses*.

While these proposals are likely to undergo a number of changes before becoming law, these discussions highlight the importance of enhancing consistency among different privacy law regimes, especially as Canada's adequacy status under the GDPR, which affords Canadian businesses handling personal data that is subject to the GDPR with a competitive advantage, is currently up for review. Furthermore, we can expect similar talks of reform concerning the Alberta *Personal Information Protection Act* (Alberta PIPA) and the British Columbia *Personal Information Protection Act* (BC PIPA), which, in addition to the Québec Private Sector Act, are deemed "substantially similar" to PIPEDA and therefore apply in lieu thereof for intra-provincial privacy matters.

Enforcement

The CPPA will bring major changes to the federal privacy enforcement regime and create significant compliance risks for businesses. Most notably, the CPPA will grant new order-making powers to the Commissioner, and enable the Commissioner to make recommendations to the Tribunal for the imposition of penalties of up to C$10,000,000 or 3 per cent of the organization's global gross revenues, whichever is higher. In contrast, equivalent fines use a cap of 2 per cent under the GDPR and Québec Bill 64. Further, the most egregious CPPA violations would constitute offences punishable, upon prosecution, with a fine up to C$25,000,000 or 5 per cent of the organization's global gross revenues. This is an upper

limit that is higher than the one currently provided under either the GDPR or Québec Bill 64, which is capped at 4 per cent (although Québec Bill 64 provides for the doubling of fines for subsequent offences).

Powers of the Commissioner

Current powers maintained – investigations, compliance agreements and audits. As under the current regime, the CPPA provides that individuals may file complaints or the Commissioner can initiate a complaint on its own initiative (s. 82 CPPA replacing s. 11 PIPEDA). The Commissioner maintains the following powers:

- Carrying out investigations in respect of a complaint (s. 83 CPPA replacing s. 12 PIPEDA);
- Entering into compliance agreements with organizations who have contravened the statute (s. 86 CPPA replacing s. 17.1 PIPEDA); and
- Conducting audits regarding an organization's compliance with the statute (s. 96 CPPA replacing s. 18 PIPEDA).

New powers – compliance orders and recommendations of penalties. The CPPA will grant the Commissioner new powers to conduct an inquiry after investigating a complaint (s. 88) or in respect of the non-compliance with a compliance agreement (s. 89). Following an inquiry, the Commissioner will have to render a decision and, if the Commissioner finds that organization has contravened the CPPA, it will be able to issue a compliance order or a recommendation that the Tribunal impose a penalty (s. 92).

- **Compliance orders.** The CPPA would grant the Commissioner significant new powers to order organizations to do the following:
    - Take measures to comply with the statute;
    - Stop doing something that is in contravention of the statute;
    - Comply with a compliance agreement; and
    - Make public any measures to correct its policies, practices or procedures (s. 92(2)).

  An organization will be able to appeal a compliance order to the Tribunal, as discussed below. If it is not appealed, it will be enforceable in the same manner as an order of the Federal Court (s. 103).

- **Penalty recommendation.** Unlike privacy regulators under other regimes (*e.g.*, the GDPR and Québec Bill 64), the Commissioner will not have powers to directly impose penalties for CPPA violations. However, the Commissioner will have powers to make a recommendation to the Tribunal that it impose a fine on the organization for violating the CPPA's key provisions (s. 93).

Monetary penalties imposed by the Tribunal

The CPPA will grant the Tribunal powers to impose a penalty on an organization after giving the organization and the Commissioner the opportunity to make representations (s. 94(1)). The Tribunal may rely on either the Commissioner's findings or its own findings (s. 94(2)). Significantly, organizations will have a defence of due diligence (s. 94(3)). This is a notable distinction from the regime currently proposed under Québec Bill 64, which does not provide an equivalent defence.

The maximum penalty for all the contraventions in a recommendation taken together is the higher of C$10,000,000 and 3 per cent of the organization's gross global revenue in its financial year before the one

in which the penalty is imposed (s. 94(4)). The statute sets out the factors that the Tribunal must consider in determining the amount of the penalty (s. 95(5)).

Appeals to the Tribunal

The CPPA will also grant complainants and organizations a right to appeal before the Tribunal (s. 100) any decision issued by the Commissioner in which it finds that the organization has contravened, or not, the CPPA. This will also extend to any compliance order issued by the Commissioner against the organization and any decision issued by the Commissioner in which it decides not to recommend the imposition of a penalty.

Offences

Certain more egregious conduct could constitute an offence leading to a fine of a maximum of the higher of C$25,000,000 and 5 per cent of the organization's gross global revenue in its previous financial year (s. 125). Such as for offences provided under section 28 of PIPEDA, these offences would be prosecuted by the Attorney General of Canada.

The following will constitute an offence under section 125 of the CPPA:

- Knowingly contravening the breach reporting and notification requirements (s. 58), including record-keeping requirements (s. 60(1));
- Knowingly contravening the requirement to retain personal information that is subject to an access request (s. 69);
- Knowingly using de-identified information to identify an individual (s. 75);
- Knowingly contravening a compliance order issued by the Commissioner; and
- Obstructing the Commissioner in the investigation of a complaint, in conducting an inquiry or in carrying out an audit.

Private right of action

The CPPA will introduce a new private right of action by which an individual affected by a CPPA contravention may bring a claim against the organization for damages for loss or injury suffered as a result of the contravention, provided that:

- The Commissioner finds that the organization has contravened the CPPA and the finding may no longer be appealed, either because the time limit to appeal has expired or the Tribunal has dismissed a prior appeal; or
- The Tribunal finds that the organization has contravened the CPPA.

An individual affected by a contravention of the offences set out in CPPA (*e.g.*, failing to report to the Commissioner, maintain records or certain information; penalizing an employee for reporting a CPPA contravention; or using de-identified information to identify an individual) may also bring a claim against the organization. In each case, a limitation period of two years after the date of the Commissioner's finding, the Tribunal's decision or conviction of a CPPA offence (as applicable) applies.

By way of comparison, Québec Bill 64's private right of action is broader than the one proposed under the CPPA, as it does not require a prior finding of contravention to the CPPA or a conviction for an offence in order to bring a claim for damages. Another important distinction is the fact that Québec Bill 64 grants plaintiffs punitive damages of at least C$1,000 for an infringement that is intentional or results from a gross fault, meaning that a plaintiff may not have to establish the existence of compensable harm under Québec Bill 64's private right of action.

Whistleblowing and anti-reprisal provisions

The CPPA will include a whistleblowing provision that is the same as the provision currently included in PIPEDA (s. 123 CPPA replacing s. 27 PIPEDA). The Commissioner has used information received under this provision to initiate a complaint on at least one occasion (PIPEDA Case Summary #310). Similarly, the CPPA will include an anti-reprisal provision that is the same as the provision currently included in PIPEDA (s. 124 CPPA replacing s. 27.1 PIPEDA).

Codes of practice and certification programs

Sections 76 and 77 of the CPPA will bring in new provisions to enable the creation of "codes of practice" and "certification programs", a means of encouraging voluntary, sectoral practices that favour privacy protection. Similar provisions are included in Articles 40 to 43 of the GDPR and may provide for greater certainty in the application of the CPPA.

The CPPA will allow any organization and other "entities" (whether or not subject to the CPPA and including government institutions) to seek the Commissioner's approval of codes of practice and certification programs. Organizations may choose to voluntarily comply and maintain certification as a business measure. Doing so will not necessarily be proof of compliance with the CPPA, though the Commissioner has discretion to decline to investigate certified organizations (s. 83(1)(d)) and is prohibited from recommending that a penalty be imposed against an organization "if the Commissioner is of the opinion that, at the time of the contravention of the provision in question, the organization was in compliance with the requirements of [an approved] certification program (s. 93(3))".

Accountability

In sections 7 through 11, the CPPA codifies and elaborates on the Principle of Accountability currently articulated in Schedule 1 of PIPEDA. While the changes to current requirements appear relatively limited, some notable additions under the CPPA will likely enhance the clarity of those requirements for businesses.

In light of Québec Bill 64, it is notable that the CPPA is silent about the obligation to conduct a privacy impact assessment in certain circumstances and a "privacy by design" requirement, both of which appear to play an important role under the proposed Québec privacy regime.

Notion of control

As under PIPEDA, the CPPA continues to provide that an organization is accountable for personal information that is under its control (s. 7(1) CPPA replacing Principle 4.1 PIPEDA). However, the CPPA will go further by defining the notion of "control", stating that personal information "is under the control of the organization that decides to collect it and that determines the purposes for its collection, use or disclosure" (s. 7(2) CPPA). Like PIPEDA, the CPPA reiterates that control rests with the organization even when the information has been transferred to a service provider (s. 7(2) CPPA replacing Principle 4.1.3 PIPEDA). Similarly to the GDPR, the CPPA distinguishes the obligations applicable to organizations in

control and service providers, the latter not being subject to Part I of the Bill except for section 57 (security safeguards) and section 61 (notification to customer in case of a breach).

Role of the privacy officer

The CPPA also echoes the PIPEDA requirement that an organization must designate an individual "to be responsible for matters related to its obligations" under the CPPA (s. 8 CPPA replacing Principle 4.1.1 PIPEDA) and provide the designated individual's business contact information to any person who requests it (s. 8 CPPA replacing Principle 4.1.2 PIPEDA). Unlike Québec Bill 64, which attributes this role to "the person exercising the highest authority" within the organization (*i.e.*, the CEO) by default, the CPPA does not specify who within the organization must fulfill this role.

Privacy management program

CPPA will require each organization to implement a "privacy management program" that includes (but presumably is not limited to) the policies, practices, and procedures the organization implements to fulfil its CPPA obligations. The required subject matter of these policies is generally the same as under PIPEDA: they must address the protection of personal information, the handling of inquiries and complaints, the training of staff on policies and procedures, and the development of materials to explain the policies and procedures (s. 9 CPPA replacing Principle 4.1.4 PIPEDA). Notably, the CPPA will introduce a new requirement that an organization, when developing its privacy management program, consider the volume and sensitivity of the personal information under its control (s. 9(2) CPPA). This is likely intended to reinforce the Commissioner's longstanding message that organizations' policies and safeguards need to be reasonable having regard to the types of information they handle.

The CPPA will also require an organization must give the Commissioner access to its policies and procedures upon request (s. 10 CPPA). Although PIPEDA does not contain an equivalent requirement, organizations have generally provided such materials to the Commissioner in any event, therefore, this provision likely changes little as a practical matter.

Unlike Québec Bill 64, which requires organizations to publish equivalent internal policies and procedures on its website or, if the organization does not have a website, by any other appropriate means, CPPA does not appear to impose a similar requirement with respect to its privacy management program.

Record of purposes

Additionally, section 12(3) of the CPPA will require an organization to identify and record each of the purposes for which it collects, uses, or discloses any personal information, and that it do so at or before the time of collection. In this respect, the CPPA appears to go beyond PIPEDA, which requires that organizations document only the purposes of collection (Principle 4.2.1 PIPEDA).

Consent

While the notion of consent has only been slightly updated under the CPPA, the proposal promises to introduce new consent exception for a collection or use of personal information for various types of business activities (see section "Legitimate business activity" below for details). The intent behind this new consent exception appears to be to enhance the meaningfulness of the notion of consent by reducing the number of situations in which it must be sought, thereby mitigating the risk of "consent fatigue".

It bears noting that, unlike Québec Bill 64, the CPPA does not directly address requirements pertaining to the handling of a children data.

This section summarizes the PIPEDA consent requirements that remain unchanged or that were slightly updated under the CPPA, and discusses the new consent exceptions introduced by the CPPA.

Updated PIPEDA consent requirements

Principle 4.3 of Schedule 1 of PIPEDA is replaced by section 15 of the CPPA which provides, similarly to PIPEDA, that an organization must obtain an individual's valid consent for the collection, use or disclosure of the individual's personal information unless otherwise provided by the law (s. 15(1)). It also provides that the individual's consent must be obtained at or before the time of the collection of personal information or, if the information is to be used or disclosed for a new purpose, before the information is used or disclosed for this new purpose (s. 15 (2)).

Form of consent. The form of consent remains unchanged under the CPPA, as it must be expressly obtained, 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 (s. 15 (4) replacing Principles 4.3.4, 4.3.5 and 4.3.6 PIPEDA).

Valid consent. For consent to be valid, the CPPA, inspired by the recently published *Guidelines for obtaining meaningful consent*, requires an organization to provide the individual with certain information in "plain language". The information to be provided seems to be aligned with that typically included in a privacy notice:

- The specific type of personal information collected, used or disclosed;
- The purposes for the collection, use or disclosure;
- The way in which the information is collected, used or disclosed;
- Any reasonably foreseeable consequences of the collection, use or disclosure; and
- The names of any third parties or types of third parties to which the organization may disclose the personal information (s. 15 (3) CPPA replacing Principle 4.3.2 and section 6.1 PIPEDA).

It should be noted that this last requirement (*i.e.*, disclosing the names of third parties) does not apply to service providers since the CPPA states that a transfer to a service provider can take place without the knowledge or consent of individuals (s. 19).

Limiting collection and withdrawing consent. Other PIPEDA consent requirements remain unchanged. This includes the requirement to only collect information required to provide the product or service (s. 15(5) CPPA replacing Principle 4.3.3 PIPEDA); the requirement not to use deceptive or misleading practices to obtain consent (s. 16 CPPA replacing Principle 4.4.2 PIPEDA); and requirements relating to the withdrawal of consent (s. 17(1) and (2) CPPA replacing Principle 4.3.8 PIPEDA).

New consent exceptions

Many of the PIPEDA consent exceptions remain in the CPPA. This includes the employment relationship consent exception (s. 24 CPPA replacing s. 7.3 PIPEDA), the work product consent exception (s. 23 CPPA replacing s. 7(1)(b.2) PIPEDA) and the business transaction consent exception (s. 22(1) CPPA replacing s. 7.2(1) PIPEDA), although there is a new requirement that the information be de-identified before it is used or disclosed until the transaction is completed (s. 22(1)(a)). It is unclear whether this last requirement is realistic in all circumstances (*e.g.*, in some situations, the purchaser may wish to validate the identity of

certain key employees before deciding to complete the transaction). It is also unclear how the business transaction exception will interact with the new CPPA consent exception provided when an organization is carrying a due diligence exercise to prevent or reduce its commercial risk (s. 18(2)(b)).

The CPPA provides for the following new consent exceptions:

Legitimate business activity. The CPPA provides a new consent exception for a collection or use of personal information if:

- It falls within the list of business activities detailed below;
- A reasonable person would expect such a collection or use for the business activity; and
- The personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions (s. 18(1)).

The list of business activities covered by this consent exception are activities:

- Necessary to provide or deliver a product or service that the individual has requested from the organization;
- Carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk;
- Necessary for the organization's information, system or network security;
- Necessary for the safety of a product or service that the organization provides or delivers;
- 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; or
- Any other prescribed activity (s. 18(2)).

Socially beneficial purposes. The CPPA introduces a new exception for disclosing personal information that has been de-identified without consent for a socially beneficial purpose to a government institution (or part of a government institution in Canada), a health care institution, post-secondary educational institution or public library in Canada or to any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada (s. 39(1)). The notion of "socially beneficial purpose" is defined in the CPPA as a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose (s. 39(2)).

Research and statistics. The CPPA also provides new consent exceptions for the use of de-identified personal information (s. 20) as well as for the organization's internal research and development purposes upon the information being de-identified (s. 21), as further discussed in the section below entitled "Research and analytics."

Reasonableness test (appropriate purpose)

PIPEDA includes a catchall reasonableness test (*i.e.*, the "reasonable person" test), which dictates the limits of its application and which may apply even if consent was obtained from individuals. The CPPA includes this same requirement under which an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances (s. 12(1) CPPA replacing s. 5(3) PIPEDA).

The CPPA provides the factors that must be taken into account in determining whether the purposes are appropriate. These factors are largely the same as the those elaborated in the *Turner v. Telus Communications Inc.* decision in which the Federal Court, and subsequently affirmed by the Federal Court of Appeal, set out the factors for evaluating whether an organization's purpose was in compliance with subsection 5(3). These factors are:

- The sensitivity of the personal information;
- Whether the purposes represent legitimate business needs of the organization;
- The effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;
- Whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and
- Whether the individual's loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual (s. 12(2) CPPA).

Since the wording of the new provision is similar to the one used under PIPEDA, the *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* document published by the Commissioner in May 2018 may still be relevant.

Individual rights

Similarly to PIPEDA, the CPPA will grant individuals the right to access and amend (correct) their personal information. It will also create a new right to have personal information disposed (deleted) and to have it moved from one organization to the other under limited circumstances.

Right to access and amend

The rights to access and amend personal information are detailed in sections 63 to 71 of the CPPA.

Overall, the CPPA will not modify the previous regime (sections 8 and 9 and Principle 4.9 PIPEDA).

Disclosures to third parties. As under PIPEDA, upon a written request from an individual, an organization will be required to inform him/her whether it holds any personal information about him/her, how it used it and, when it had disclosed such information, provide the name of the third parties or types of third parties to whom the disclosure was made (including when such disclosure was made without consent). We note that the CPPA does not provide an exception to this last requirement, whereas under PIPEDA, an organization may, when it is not possible to provide an accurate list of third parties, provide a list of

organizations to which it may have disclosed such personal information (section 63(1) and (2) CPPA replacing Principle 4.9.3 PIPEDA).

Amendment and record of disagreement. Once an individual is granted access to their personal information, if they demonstrate that their personal information is inaccurate, outdated or incomplete, the CPPA maintains PIPEDA requirement to amend such information and to inform any third party that has access to such information about the amendment. If the organization disagrees with the requested amendments, it must keep a record of the disagreement and inform third parties about such disagreement (section 71 and 71(3) CPPA replacing Principles 4.9.5 and 4.9.6 PIPEDA).

Retention of information used for decision-making. As under PIPEDA, the CPPA will require the organization to retain the information for a sufficient period of time to permit the individual to make a request to access or amend his/her personal information (s. 69 CPPA replacing s. 8(8) PIPEDA) or to be informed about automated decision-making (see below). This retention period will be set at six months from the date of the refusal to grant the request (or failure to respond to such request), but the Commissioner can decide to extend this period (s. 54 and 82(3) CPPA).

Right to be informed of automated decision-making systems

The CPPA will grant individuals, at section 63(3), a new right to receive an explanation about the use of an automated decision system to make a prediction, recommendation or decision about them and of how personal information was used to that effect. Contrary to Québec Bill 64 and the GDPR however, the CPPA will not grant individuals with the right to object to such use or to have the decision reviewed by an employee of the organization (for more information on the CPPA's provisions regarding automated decision-making systems, see section entitled "Research and analytics" above).

Right to disposal

Section 55 of the CPPA will create a clear right for individuals to have their personal information disposed (*i.e.*, permanently and irreversibly deleted) by an organization in control upon request. This right applies to any personal information collected from the individual (*i.e.*, not from third parties). Grounds for refusing such disposal, which will have to be detailed by the organization in its written response to the requesting individual, will be limited to situations where it would result in disposing of information about another individual or where federal, provincial or contractual requirements would prevent the organization from doing so. In situations where the organization has transferred the information to a service provider, it will be required to inform it of the disposal request and obtain a written confirmation from such provider that it has also disposed of the information.

It is worth noting that this right to disposal does not appear to encompass a right to de-indexation or right to be forgotten, contrary to Québec Bill 64 and the GDPR.

Right to mobility

The CPPA innovates at section 72 by creating a limited right to data portability, which will allow individuals to request from an organization in control that their personal information be disclosed to another organization (s)he designates if both organizations are subject to a "data mobility framework" provided under the regulations. This right will only apply to personal information collected from individuals (*i.e.*, not from third parties). The data mobility frameworks to be created through regulation will have to include safeguards for the secure disclosure of information and parameters for the technical means for ensuring interoperability (s. 120). They will also have to specify the organizations subject to the framework, which will likely belong to specific industry sectors such as open banking or telecommunications. Here again, the

CPPA will be more limited in scope than Québec Bill 64 and the GDPR, as it refrains from opening the door to general portability requests aimed at organizations that may not be involved in any interoperability scheme or subject to specific competition requirements.

Research and analytics

The CPPA will introduce a definition of "de-identified" information, which albeit not expressly excluded from the scope of "personal information", meaning that it may still be subject to Canadian privacy law requirements, will allow organizations to benefit from greater flexibility with respect to processing such de-identified information, including for internal research and development purposes. Furthermore, the CPPA will also include provisions concerning the use of "automated decision systems", which aim to enhance transparency.

De-identification

The CPPA will take an approach to anonymization and de-identification that differs both from its predecessor, PIPEDA (which does not mention de-identification and makes only passing reference to anonymization as an alternative to destruction), and the new Québec Bill 64, which introduces a clear separation between de-identified information and anonymized information. Under the CPPA, to "de-identify" 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" (s. 2). Anonymization will fall within this definition, creating information that does not identify an individual from personal information. However, it appears that the definition will also allow for less rigorous forms of de-identification, which might include such techniques as pseudonymization, tokenization or cryptographic hashing, provided those lesser varieties of de-identification could not be used to re-identify an individual in reasonably foreseeable circumstances.

Further evidence that the CPPA will recognize forms of de-identification less rigorous than anonymization can be found in CPPA sections 74 and 75. Section 74 states that an organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information; section 75 states that an organization must not use de-identified information alone or in combination with other information to identify an individual, except in order to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information. Moreover, organizations that knowingly contravene section 75 are liable to a fine of up to the higher of $25,000,000 or 5 per cent of the organization's gross global revenue (s. 125(a)). These sections implicitly recognize the inherent risk of re-identification associated with forms of de-identified data that fall short of true anonymity.

How the clause "could not be used to re-identify an individual in reasonably foreseeable circumstances" should be interpreted remains to be seen, but given other provisions of the CPPA, it may need to be treated as providing a degree of flexibility favourable to organizations. For example, in the new section addressing prospective business transactions (s. 22), parties to a prospective business transaction may use and disclose an individual's personal information without their knowledge or consent if the information is de-identified before it is used or disclosed. Typically, in prospective transactions, the seller will provide the buyer with information about employees as part of the due diligence process. While direct identifiers and some indirect identifiers may be redacted in such circumstances, there are limits, and aggregation is impractical.

Importantly, the CPPA will provide that the act of de-identifying personal information is a use of personal information that does not require the knowledge or consent of individuals, resolving a long-standing ambiguity under PIPEDA.

Finally, as may be evident from the sections discussed above, de-identified information will be subject to the CPPA. Arguably, as defined, even truly anonymized information (*i.e.*, information created from personal information that does not identify an individual) will be subject to the CPPA, although the risk of falling afoul of obligations such as those set out at sections 74 and 75 when using truly anonymized information will likely be low.

Research

The CPPA will introduce a new consent exception that will allow the use of personal information for an organization's internal research and development purposes, if the information is de-identified before it is used (s. 21). Similar to Québec Bill 64, the CPPA thereby will permit organizations to re-use information collected for one purpose for secondary research purposes, such as enterprise or business analytics. Using such information to train machine learning systems will arguably also fall within the "research and development" contemplated by this exception.

Automated decision systems

The CPPA will introduce several provisions that refer to the use of automated decision systems, which are defined as "technology that assists or replaces the judgment of human decision makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets". The CPPA will invoke the defined term in two contexts, "Openness and Transparency" (s. 62 CPPA) and "Access to and Amendment of Personal Information" (s. 63-71 CPPA).

Under Openness and Transparency, an organization using an automated decision system will be obliged to make readily available, in plain language, a general account of the organization's use of such a system to make predictions, recommendations or decisions about individuals that could have significant impacts on them (s. 62(2)(c)). While "significant impacts" is not defined or elucidated, one natural interpretation could include some of the circumstances that risk giving rise to significant harm as that term is defined under section 58(7), such as circumstances involving reputation, employment, finances or credit.

Under Access to and Amendment of Personal Information, if an organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization will be required, on request by the individual, to provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained (s. 63(1)(3)).

This obligation to explain may be rendered particularly challenging by the additional requirement set out in section 66(1), which obliges the organization to provide this information to the individual in plain language. Whereas the plain language requirement set out in the provisions governing openness and transparency will be satisfied by giving "a general account", it is not clear whether a plain language explanation of a given prediction, recommendation or decision can be given when the system used is based on machine learning, deep learning or neural nets. The CPPA does not provide individuals with any further rights beyond the right to an explanation. For example, in contrast to Québec Bill 64, individuals cannot submit observations to a staff member in a position to review a decision. Moreover, the CPPA provisions that will permit individuals to have information amended if they can demonstrate that the information is not accurate, up-to-date or complete (s. 71(1)) do not provide a clear foundation for challenging the conclusions reached by an automated decision system.

Outsourcing and cross-border

The CPPA will not materially alter outsourcing or cross-border requirements. Rather, it will formally incorporate existing requirements and best practices, and formally distinguish between the role and obligations of the service provider and the organization that has personal information under its control. For businesses, these changes will likely be welcome in that they will provide greater clarity and consistency.

Outsourcing

The CPPA will provide welcome clarity with respect to the transfer of personal information to a service provider, which the CPPA defines as "an organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor, which provides services for or on behalf of another organization to assist the organization in fulfilling its purpose" (s. 2).

Significantly, section 19 of the CPPA will expressly permit organizations to transfer personal information to a third party service provider without knowledge or consent, providing a definitive conclusion to a tumultuous few years in which the Commissioner adopted, and subsequently reversed, the policy position that the transfer of personal information for processing required additional, express consent.

Lastly, the CPPA will elucidate the following additional principles that apply to outsourcing:

- The CPPA deems personal information collected, used or disclosed on behalf of an organization by a service provider to be under the control of the organization (not the service provider) if the organization determines the purposes of collection, use or disclosure (s. 7(2));

- As with PIPEDA, the CPPA imposes accountability on an organization that transfers personal information to a third party service provider to ensure (by contract or otherwise) that the service provider provides similar protection over that personal information (s. 11(1));

- The CPPA clarifies that the obligations set out in the CPPA do not apply to a service provider to the extent that an organization transfers personal information to it for processing. If the service provider collects, uses or discloses personal information for any other purpose, then Part 1 of the CPPA applies (s. 11(2));

- If an organization disposes of personal information upon request by an individual, the CPPA requires the organization to notify and confirm its service providers do the same (s. 55(3)); and

- The CPPA imposes notification obligations on a service provider that suffers a data breach (s. 61; see the "Safeguarding and incident response" section for more information).

It is also worth noting, by way of comparison, that Québec Bill 64 incorporates similar requirements with respect to outsourcing, although its requirements with respect to the content of outsourcing agreements are more prescriptive than under the CPPA.

Cross-border transfers and cooperation

Contrary to Québec Bill 64 and the GDPR, which provide for an evaluation of the foreign privacy framework's level of equivalency, but in line with PIPEDA and past guidance from the Commissioner, the CPPA does not contain any restriction to the transfer of personal information outside of Canada.

Transparency. The only requirement found in the CPPA at section 62(2)(d) is a transparency one: the privacy policy to be made available by organizations will have to include details as to whether or not the organization carries on any international or interprovincial transfer or disclosure of personal information but only to the extent such transfer or disclosure may have reasonably foreseeable privacy implications. This last portion of the requirement is unclear and seems to imply that this information must only be included where personal information is shared with an organization/entity that may not protect it adequately or may be subject to laws that are not substantially similar to the CPPA. This should be clarified.

Cooperation with foreign regulators. Acknowledging the inherent international nature of data protection efforts, section 117 of the CPPA will afford the Commissioner new powers regarding the disclosure of certain information to foreign privacy regulators. Interestingly, such powers will include the ability to enter into cooperation agreements with foreign regulators, which may involve cooperation for enforcing foreign data protection laws, developing guidance, undertaking and publishing research, sharing expertise and identifying issues of mutual interest.

Safeguards and incident response

The CPPA will include a security-safeguarding obligation that is very similar to that now in effect under PIPEDA – an obligation to protect personal information through "proportionate" physical, organizational and technological security safeguards (s. 57(1)). Sensitivity will become the new primary factor governing the adequacy of security safeguards, though "the quantity, distribution, format and method of storage of the information" will continue to be relevant (s. 57(2)).

The CPPA will preserve the notification and reporting requirements that apply to "breach of security" safeguards as they exist today. Namely:

- The "breach of security safeguards" definition is unaltered;
- The CPPA will continue to require reporting to the Commissioner and individual notification;
- The standard for reporting and notification will continue to be the "real risk of significant harm" standard;
- The time requirement for reporting and notification will continue to be "as soon as feasible"; and
- There will continue to be a requirement to notify other organizations who are believed to have an ability to reduce the risk of harm or mitigate harm.

The only new requirement is that service providers will become obligated under the CPPA to notify their customers as soon as feasible after "determin[ing] that a breach of security safeguards has occurred" (s. 61). This change will establish a statutory minimum for service provider notification, a matter typically governed by the terms of service provider agreements. The chosen trigger for notification – a "determination" – will give vendors time to investigate security incidents before notifying.

Next steps

It is notable that the federal government has not provided any indication with respect to the timeline for adopting its proposal nor with respect to the transition period that will be afforded to businesses, once Bill C-11 is enacted, in order to adapt their practices before being exposed to new and potential onerous

enforcement mechanisms. However, as the proposal contemplates a considerable increase in penalties, it is likely that the government will hold consultations and hearings in order to obtain the input of stakeholders, as was recently the case in Québec with respect to Bill 64 (see "*Summary of special consultations and public hearings on Québec's Bill 64*" for more detail).

Author(s)

Eloïse Gratton **Elisa Henry** **François Joli-Coeur** **Max Jarvie**

Daniel Michaluk **Katherine McNeil** **Andy Nagy** **Ira Parghi**

Service(s)

Cybersecurity, Privacy & Data Protection