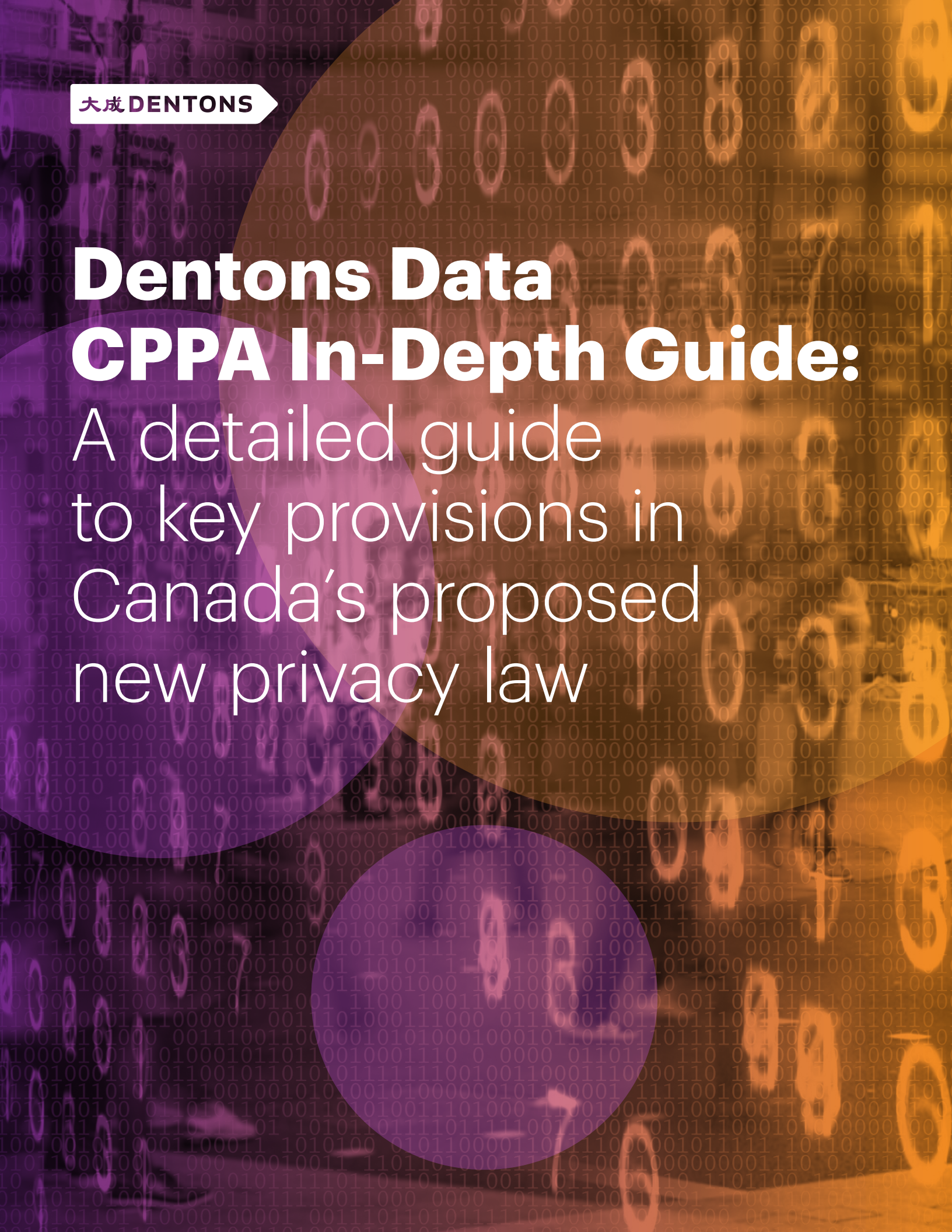
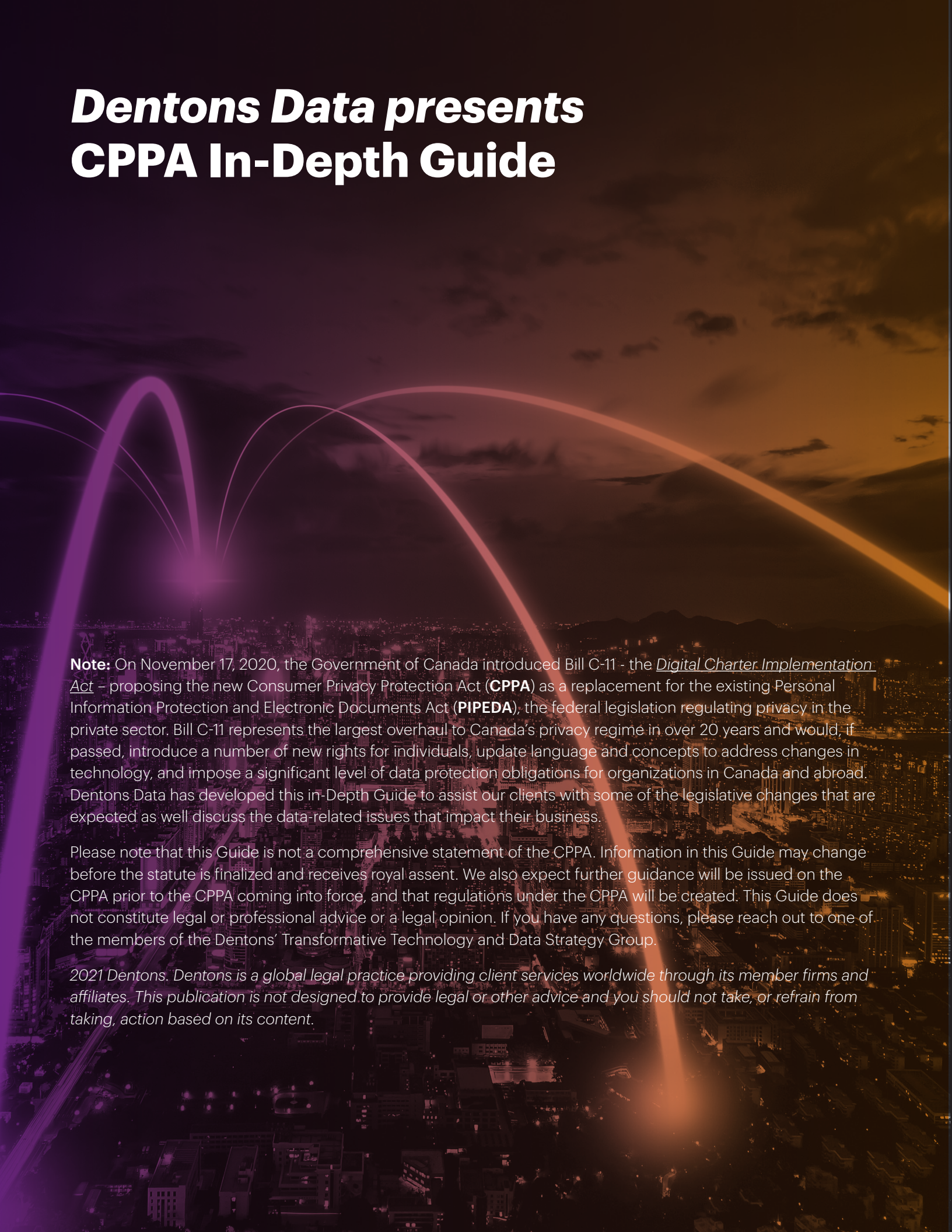
大成 DENTONS

Dentons Data CPPA In-Depth Guide:

A detailed guide to key provisions in Canada's proposed new privacy law



Dentons Data presents
CPPA In-Depth Guide

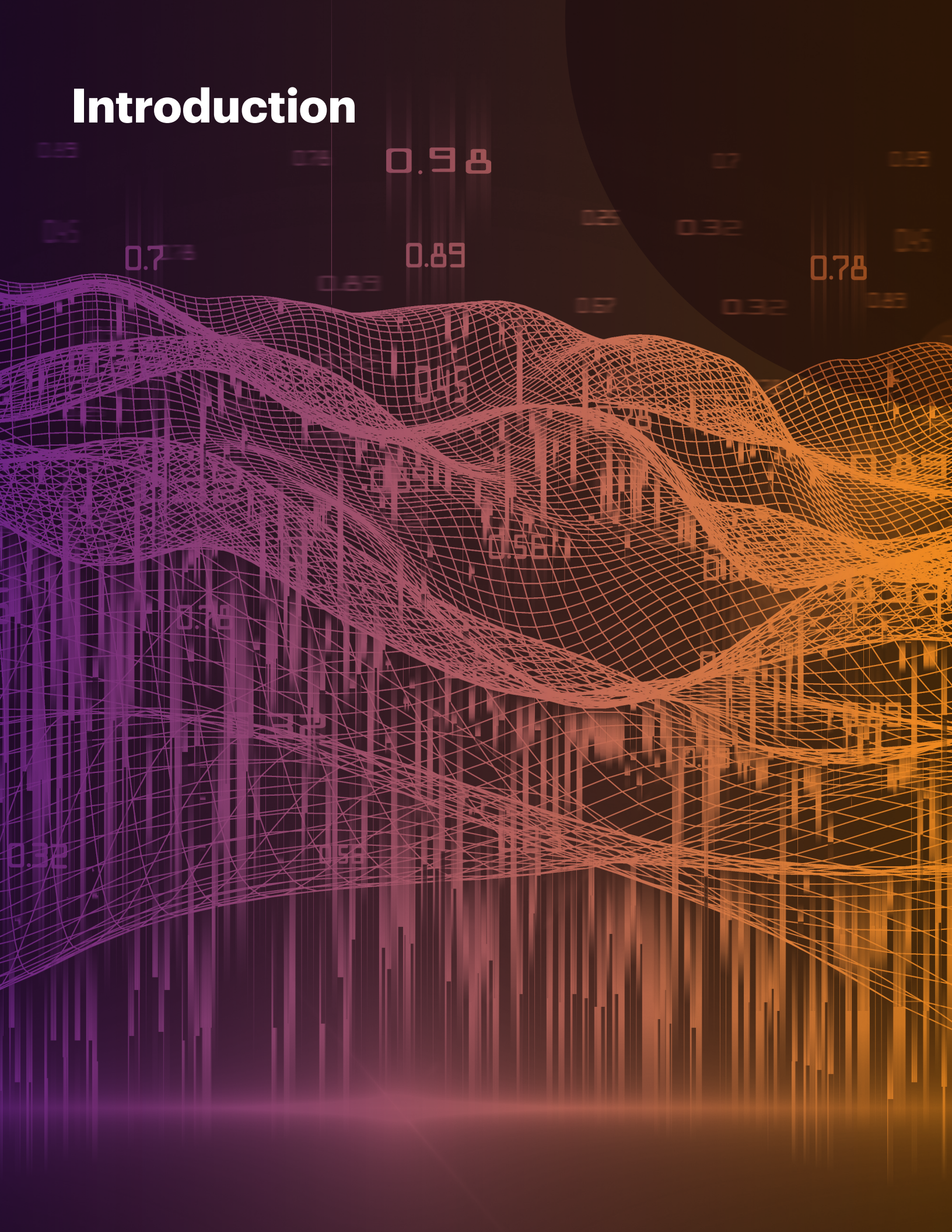


Note: On November 17, 2020, the Government of Canada introduced Bill C-11 - the *Digital Charter Implementation Act* – proposing the new Consumer Privacy Protection Act (**CPPA**) as a replacement for the existing Personal Information Protection and Electronic Documents Act (**PIPEDA**), the federal legislation regulating privacy in the private sector. Bill C-11 represents the largest overhaul to Canada's privacy regime in over 20 years and would, if passed, introduce a number of new rights for individuals, update language and concepts to address changes in technology, and impose a significant level of data protection obligations for organizations in Canada and abroad. Dentons Data has developed this in-Depth Guide to assist our clients with some of the legislative changes that are expected as well discuss the data-related issues that impact their business.

Please note that this Guide is not a comprehensive statement of the CPPA. Information in this Guide may change before the statute is finalized and receives royal assent. We also expect further guidance will be issued on the CPPA prior to the CPPA coming into force, and that regulations under the CPPA will be created. This Guide does not constitute legal or professional advice or a legal opinion. If you have any questions, please reach out to one of the members of the Dentons' Transformative Technology and Data Strategy Group.

Contents

Introduction



Since January 1, 2001, Canada's *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), has been Canada's primary statute governing how private sector organizations collect, use, disclose and safeguard personal information. On November 17, 2020, the Government of Canada introduced Bill C-11 - the *Digital Charter Implementation Act* – proposing the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for data protection sections of PIPEDA.

Purpose of the Guide

The purpose of this Guide is to highlight some of the main principles and changes proposed by Bill C-11, and the likely impacts they will have on businesses. It is meant as a business aid for our clients who wish to understand, in depth, the expected changes. This Guide is not a comprehensive statement of Bill C-11, and some of the content in this Guide may change as the language in Bill C-11 is finalized.

Scope of the CPPA

Bill C-11 consists of two parts – Part 1, which would enact the new CPPA, and Part 2, which would enact the legislation to establish the Personal Information and Data Protection Tribunal (**Tribunal**). It also incorporates previous amendments made to PIPEDA in 2015 via the *Digital Privacy Act*. The current PIPEDA would continue to exist, but it would be focused on the electronic documents aspect of e-commerce that are currently found in Part 2 of that legislation.

Notably, PIPEDA's Schedule 1 Principles (based on the Organization for Economic Co-operation and Development Principles) would be gone, incorporated into the statutory language of the proposed CPPA. The Schedule 1 language of recommendation (i.e., "should") has, in its transposition into the CPPA, been replaced with mandatory language (i.e., "must"). The CPPA would still contain the balancing language found in PIPEDA – where the stated goal is "to support and promote electronic commerce" by protecting personal information. As with PIPEDA, the scope of the CPPA is limited the collection, use, and disclosure of personal information "in the course of commercial activities".

New key definitions

There are several new definitions, which would have an impact on businesses and their privacy practices.

The term "commercial activity", which goes to the core of the scope of the statute, is now further defined and qualified. It would mean (as it does in PIPEDA) "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character". However, under the CPPA, this would be qualified by adding "taking into account an organization's objectives for carrying out the transaction, act or conduct, the context in which it takes place, the persons involved and its outcome." This contextual and holistic approach potentially encompasses a broader swath of activities than currently captured by PIPEDA.

"Automated decision systems" would be brought into the ambit of the CPPA, and they are defined as being "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". This is an expansive definition, and organizations will likely want to understand better what exactly is encompassed by the phrase "assists or replaces" humans.

The CPPA would also add a definition of what it means to de-identify personal information. Under the CPPA, "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". This is one of the most concerning proposals to organizations and legal experts as the CPPA would not carve out anonymized data from the scope of the statute. We discuss how the proposed approach is a marked departure from other privacy laws, including the General Data Protection Regulations (UK GDPR and EU GDPR; collectively, GDPR), as well hampers an organization's innovative abilities since personal information, even when de-identified, remains caught by the statute.

The controller / processor distinction is not formally recognized in PIPEDA as it is, for example, in the General Data Protection Regulations. The terms "controller" and "processor" are not defined under PIPEDA. Rather, PIPEDA refers to "organizations" as a more general concept, which includes both controllers and processors. The CPPA would define the term "service provider" to mean 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 purposes". While many organizations will welcome the clarity, there are likely others that will be surprised to find themselves caught by this definition, in particular parent corporations and affiliates.

Mandatory privacy management programs

The CPPA would require that every organization implement a "privacy management program", which must include policies, practices and procedures that it puts in place to fulfil its obligations, including those pertaining to the protection of personal information. Explanatory materials, training for staff and processes to manage requests to access personal information are also required. Organizations would be required to take into account both the sensitivity and the volume of the personal information under the organization's control in developing its privacy management program. Importantly, organizations would be required to give the Office of the Privacy Commissioner of Canada (**OPC**) with access to the policies, practices and procedures that are included in their privacy management program, should the OPC request them.

Still a consent based regime

With few exceptions, PIPEDA is a consent-based privacy regime, and the CPPA is still largely consent based. Valid consent to the collection, use and disclosure of personal information would still be required, but the validity of consent is now contingent upon meeting certain meaningful consent requirements that were part of the OPC's PIPEDA guidelines, and would now be codified.

Under the CPPA, consent would have to be expressly obtained, unless an organization could establish that implied consent would be appropriate. In coming to its conclusion, the organization must take into account "the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed." This is likely to increase the documentation requirements for organizations.

Despite the renewed focus on consent, the CPPA would broaden the circumstances in which an organization is permitted to collect, use, or disclose personal information without having to provide notice or obtain consent (i.e., knowledge or consent). For example, in a marked departure from PIPEDA, but in alignment with other international privacy laws, neither knowledge nor consent would be required to collect or use personal information where it is done for one of a number of listed and defined "business activities". An important caveat to reliance on this provision is that the intended collection or use must be reasonable and expected. A notable restriction on this consent exception is that it does not apply where the personal information is "collected or used for the purpose of influencing the individual's behaviour or decisions."

While this does provide some flexibility for many businesses in respect of their ordinary and routine activities, the latter prohibition will likely have a significant impact on the ad tech industry, as it essentially forces an organization to seek consent.

Algorithmic transparency

Under the CPPA, organizations would be required to provide plain language explanations of the prediction, recommendation or decision made by automated means, and of how the personal information that was used to make the prediction, recommendation or decision was obtained. This new requirement would likely apply to organizations that have already adopted such technologies, with no grandfathering.

Data mobility would be required

The CPPA would introduce the right of an individual to request that an organization disclose the personal information that "it has collected from the individual" to an organization designated by the individual, if both organizations are subject to a data mobility framework provided under the regulations. The Governor in Council is expected to issue regulations regarding data mobility frameworks.

Creation of codes of practice and certification programs

The CPPA would contain new provisions to enable the creation of third-party codes of practice and certification programs as a means to encourage new sectoral privacy protection self-regulation. The OPC would act as an approval body for entities operating a certification program. The language of the proposed CPPA suggests that participation in these schemes is voluntary (though it is conceivable that licensing bodies could make participation in such a scheme a condition or licensing, or a membership-based organization could make participation a condition of membership). Similar to GDPR, the under the CPPA, the OPC would have the ability to approve codes of practice and certification programs. The ability to apply for such approval is not limited to "organizations" but includes all "entities," which would presumably include industry associations, interest groups and other loosely organized affiliations. Codes of practice must offer "substantially the same or greater" than the protections offered under the CPPA.

Of importance, compliance with a code of practice or a certification programs does not relieve an organization of its obligations under the CPPA.

New enforcement structure and powers

Enforcement of the CPPA would be divided between two bodies, the existing OPC as well as a new Tribunal.

Following an investigation in which the matter is not resolved, the OPC would have the power to launch an official inquiry. Unlike the PIPEDA provisions in respect of an investigation, an inquiry under the CPPA would have basic rules of evidence, the organization would have a right to be heard and be assisted by counsel, and the OPC would be required to complete an inquiry by rendering an actual decision (as opposed to a "finding" under the investigation stage). A decision, unlike a finding, is open to legal challenge. The OPC would also have limited order-making powers, as well as the ability to recommend monetary penalities to the new Tribunal (though is not able to levy such penalties directly).

One of the most significant changes to Canada's privacy landscape includes the creation of a new Tribunal that would act as an appeal body from findings, orders, or decisions made by the OPC. This is an entirely new addition to the federal privacy regime – currently no Tribunal exists. The Tribunal would be established by companion legislation to the CPPA, the *Personal Information and Data Protection Tribunal Act*. The Tribunal would determine whether to impose a penalty, and it may choose to rely on the OPC's recommendation or may substitute its own decision.

Introduction of significant monetary penalties

The CPPA would introduce significant monetary penalties. If, in completing an inquiry, the OPC finds that an organization has contravened one or more of certain listed provisions, the OPC must decide whether to recommend that a penalty be imposed on the organization by the Tribunal. The maximum penalty for all the contraventions in a recommendation taken together is the higher of CAD $10,000,000 and 3% of an organization's gross global revenue in its financial year before the one in which the penalty is imposed.

In addition, an organization that knowingly: contravenes the breach reporting provisions; contravenes the breach-related recordkeeping provisions; fails to keep personal information that is the subject of a request; attempts to re-identify de-identified information; retaliates against an employee who makes an privacy complaint; or violates an order, is:

a. guilty of an indictable offence and liable to a maximum fine of the higher of $25,000,000 and 5% of the organization's gross global revenue in its financial year; or

b. guilty of an offence punishable on summary conviction and liable to a maximum fine of the higher of $20,000,000 and 4% of the organization's gross global revenue in its financial year.

New private right of action

Finally, the CPPA would permit a a private right of action. In cases where the OPC or Tribunal has made a finding that the organization contravened the CPPA, individuals affected by the acts or omissions of an organization (these individuals do not necessarily need to be complainants) may sue the organization for damages for loss or injury.

CPPA: An in-depth look at the service provider provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

In this article, we address how the proposed CPPA would affect businesses that use service providers to process personal information, as well as those businesses acting as service providers.

The CPPA would clarify the nature of the service provider relationship

PIPEDA does not define "service provider," nor does it define what constitutes a "service provider" relationship. PIPEDA's locus of control is the organization that is responsible for information in its possession or control, which includes "information that has been transferred to a third party for processing." PIPEDA attempts to ensure the safety of personal information transferred to service providers by requiring a transferring organization to use contractual or other means to ensure the transferred information receives protection that is "comparable" to that which it provides. In addition, the service provider is only permitted to use the transferred personal information for the same purpose as that identified by the transferring organization at the time of collection.

Under the proposed CPPA, any organization providing services for or "on behalf of another organization to assist the organization in fulfilling its purposes" would be considered a "service provider." Personal information is deemed to be "under the control" of the organization "that decides to collect it and that determines the purposes for its collection, use or disclosure." This is true whether the information is collected, used or disclosed by the organization itself or by a service provider. This clarifies a problem that arose in PIPEDA where either highly integrated entities or entities working in partnership across a data supply chain (e.g., franchise or dealership business models) were mutually involved in multiple steps, leading to confusion about who was responsible for what.

Under the proposed language of the CPPA, the question of whether a service provider relationship exists would be answered with reference to which organization ultimately makes decisions about personal information. This new language adopts the conceptual basis of controller/processor found in the GDPR. Note that under the CPPA, it is possible for an organization to be a service provider for some purposes, and the accountable organization for others.

CPPA definitions of controller/service provider may disrupt existing contractual risk shifting

Businesses with an established business model may, under the CPPA, find that the accountability for personal information has been turned on its head. For instance, in a franchise-type model where personal information was collected at the franchise level, and then provided to the central franchisor, accountability under PIPEDA may well be with the franchisee. Under the CPPA, if it is the franchisor determining what is collected and how it is to be used, the franchisor may be the accountable entity, despite the actual collection occurring at the franchise level. This has implications beyond the statute – it may well disrupt existing contractual obligations in respect of breach reporting and notification, limitations of liability and indemnification provisions.

The CPPA contains a carve out from Part I for service providers, and the broader obligations under that PART would not apply to those organizations acting within the definition of service provider. However, the CPPA would provide that were a service provider to collect, use or disclose information transferred to it for any purpose other than that for which the information was transferred, it would incur all of the same obligations as any other principal organization. Businesses should be aware that any processing of personal information outside the scope of an agreement with a principal organization would likely result in the CPPA applying to them in its entirety. Under the CPPA, organizations acting as service providers will need to be very careful about how the scope of their processing activities is defined in their service contracts with principal organizations. Service providers will also need to be careful about putting in place controls to ensure that the received information is processed only within the scope agreed to.

Neither knowledge nor consent required to transfer to a service provider

The CPPA would permit organizations to "transfer an individual's personal information to a service provider without their knowledge or consent." This was an area of confusion under PIPEDA, and the subject of numerous findings by the Office of the Privacy Commissioner of Canada (**OPC**). As recently as August, 2020 the OPC noted in a finding on this point that "[o]rganizations transferring personal information to third-party processors should communicate clearly about this transfer to both current and potential customers." Under the CPPA, it appears this would not be necessary as the language of the CPPA requires neither knowledge nor consent. However, section 62(2)(d) of the CPPA would nonetheless require that an organization make readily available information about international or interprovincial transfers or disclosures if such transfers or disclosures would have "reasonably foreseeable privacy implications."

Note that under Quebec's Bill 64, which would substantially revise that province's private sector privacy law, a transfer by an organization that is "necessary for carrying out a mandate or performing a contract of enterprise or for services" is permitted without consent (section 18.3). Bill 64 is silent on whether knowledge is required.

The scope of what constitutes a "service provider" would be broadened

In addition to a contractor or subcontractor, the CPPA would define a service provider to include a parent corporation, subsidiary or affiliate providing services for or on behalf of another organization. Businesses should be aware that the processing of personal information by a related company on its behalf (as opposed to a vendor or contractor) could amount to a service provider relationship.

This has positives and negatives. On the one hand, some parent organizations may be surprised to find that, by virtue of providing back end systems and support, they may now be "service providers," and have some of the obligations that accompany that status (e.g., the obligation to notify the transferring organization of a breach of security safeguards).

On the other hand, the explicit rejection by the CPPA of the need for knowledge or consent for transfers to service providers is likely to make intracompany transfers of such information easier.

"Comparable" versus "substantially the same" – threshold for protection higher?

Like PIPEDA, the CPPA would require an organization transferring personal information to a service provider to ensure, by contractual measures or otherwise, that the transferred information is protected in the hands of the service provider. The PIPEDA requirement is that such measures provide "a comparable level of protection," while the CPPA would require that such measures provide "substantially the same protection." Is this a distinction without a difference? Arguably.

New obligations on both service provider and controlling organizations regarding disposal

If an organization were to dispose of personal information in response to an individual's request to do so (itself a new right under the CPPA), the organization is required, "as soon as feasible", to inform any service provider to which it has transferred the information of the request, and obtain confirmation from the service provider that the information had been disposed of. Implicit in this obligation is that the organization knows to what entities it has transferred the personal information at issue, which means organizations will

need to have performed (and continually update) data mapping.

As they do under PIPEDA, businesses would need to continue implementing robust contractual protections over information transferred to service providers for processing. Under the CPPA, businesses will likely want to include a requirement for service providers to track and record information disposal requests. From the perspective of service providers, they will likely want to ensure they have appropriate logging and documentation in place to provide evidence of compliance.

Service providers would be required to notify controllers about any breach affecting any personal information

Unlike PIPEDA, the CPPA would require service providers to, as soon as feasible, notify the controlling organization if "any breach of security safeguards has occurred that involves personal information."

This language casts the net very broadly, requiring service providers to notify controlling organizations of "any" breach, not just a breach which creates "a real risk of significant harm," which is the reporting and notification threshold for breaches affecting the controlling organization. Note, too, that the breach at the service provider need not involve the controlling organization's information – any breach, affecting any personal information held by the service provider, would appear to trigger the obligation. This means that, for instance, a payroll processor with 200 customers that had an employee misdirect an email to Person B containing the personal information of Person A would be required to notify all 200 of its customers of the incident.

The controlling organization would still have the gating mechanism of deciding whether such incident posed a "real risk of significant harm" and presumably report/notify on that basis. However, in the scenario provided above, the notifications from the service provider would only be relevant to one organization (the one having the information under its "control" as that is the one that has the reporting obligation to the OPC and notification obligation to affected individuals). Query the utility of having 199 other organizations receive notices from a service provider. Furthermore, requiring this creates a risk of secondary breach, in the event the service provider inadvertently includes identifiable information in its 200 notifications.

Note that under Quebec's Bill 64, a similar obligation (section 18.3(2)) would be triggered where the service provider becomes aware of "any violation or attempted violation by any person of any obligation concerning the confidentiality of the information communicated." There is similarly no "real risk of significant harm" threshold and the Bill 64 provision includes not just violations, but attempted violations. Bill 64 also requires that the service provider permit the controller to conduct any verification relating to confidentiality requirements.

CPPA: An in-depth look at the enforcement and penalty provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

In this article, we address how the enforcement powers and penalties proposed by the Bill would work and what it means for businesses.

Structure

The CPPA would provide for proceedings before a tribunal (**Tribunal**) that would act as an appeal body from findings and recommendations made by the Office of the Privacy Commissioner of Canada (**OPC**). This is an entirely new addition to the federal privacy regime – currently no Tribunal exists. The Tribunal would be established by companion legislation to the CPPA, the *Personal Information and Data Protection Tribunal Act* (**PIDPTA**), which is also introduced by Bill C-11.

These structural changes are some of the most significant changes to the privacy landscape that would occur, as they are accompanied by powers to make orders requiring compliance with the CPPA and to impose significant fines.

I. New OPC enforcement powers

The new OPC enforcement powers are a marked addition to the OPC's current powers, as the OPC may not currently make orders directing compliance and has no ability to impose or recommend monetary penalties. By contrast, under the CPPA, the OPC would have the following enforcement powers:

Investigations: Similar to the current requirements under PIPEDA, under the proposed CPPA the OPC would be required to carry out an investigation in respect of a complaint filed by an individual under section 82, except in certain circumstances. These exceptions include where the OPC is of the opinion that there is another procedure provided for under law that is preferable, where the complainant should first exhaust grievance or review procedures, and where too much time has elapsed.

Under the CPPA, the OPC would also have the ability to decline to investigate a complaint on the basis that complaint raises an issue in respect of which an OPC-approved certification program applies (the ability to approve certification programs is new under the CPPA and is dealt with in a separate article). This is discretionary – the OPC may still elect to conduct an investigation notwithstanding the organization's participation in a certification program.

The goal of the investigation process is to resolve the complaint (generally via alternative dispute resolution mechanisms, such as mediation and conciliation, as in PIPEDA).

Inquiries: Inquiries are a new process under the CPPA. Under section 88 of the CPPA, the OPC may conduct an inquiry if the matter is not resolved, discontinued or diverted to alternative dispute resolution at investigation. For unresolved matters, this essentially

gives the OPC a second kick at the can (to investigate an organization further). The OPC's power to start an inquiry is discretionary.

This is an important development. Previously, where an organization did not agree with the OPC's findings or recommendations, or declined to implement the OPC's recommendations, the organization was left with little recourse to challenge such a recommendation. Typically, the issue would remain unresolved and the OPC would note publicly that the organization declined to implement its recommendations and/or did not cooperate. The OPC was thereby able to achieve a negative reputational impact on the organization. The organization had little choice but to accept this, as there was no avenue for appeal since the OPC's findings and recommendations were non-binding and therefore not capable of appeal. Judicial review was a possibility, but the chances of success were small for all but the most egregious circumstances.

Under the CPPA, unresolved complaints would go to an inquiry phase. The OPC would have broad powers in respect of an inquiry and is not bound by any rules of evidence in conducting such an inquiry (with the exception of privilege related rules). The OPC may also determine the procedure to be followed in the inquiry. However, the language of the section references "considerations of fairness and natural justice," which are not referenced at the investigation stage. The OPC must also give the complainant and the organization an opportunity to be heard and to be assisted or represented by counsel or other person – rights not explicitly available at the investigation stage.

Decisions and compliance orders: The most important expansions of the OPC's enforcement powers are set out in sections 92-93 of the CPPA. Under those provisions, the OPC may, after concluding an inquiry, issue a finding of contravention of the CPPA, and issue a compliance order. This direct order-making power is not currently available to the OPC.

In a compliance order, the OPC may order an organization to:

a. Take measures to comply with the CPPA.

b. Stop doing something that is contravention of the CPPA.

c. Comply with the terms of a compliance agreement entered into by the organization; or

d. Make public any measures taken or proposed to be taken to correct policies, practices or procedures in place to fulfill the organization's obligations under the CPPA.

Compliance orders may be appealed to the Tribunal. If not, or if the appeal is dismissed by the Tribunal, the compliance order may be made an order of the Federal Court and is enforceable in the same manner.

Monetary penalties: Under section 93 of the CPPA, the OPC would be able to make a *recommendation* that a monetary penalty be imposed on the organization by the Tribunal, which is an entity actually empowered to impose penalties after a hearing (see section 94 discussed below). In recommending the quantum of penalty, the OPC must take into account the nature and scope of the contravention, whether the organization has voluntarily paid compensation to a person affected by the contravention, the organization's history of compliance with the CPPA, and any other relevant factor. This represents a significant new power for the OPC, which currently has no power to recommend a monetary penalty. However, even under the proposed CPPA, the power to actually impose a monetary penalty is restricted to the Tribunal, as discussed below.

As mentioned above, one of the factors that the OPC must consider is whether the organization has voluntarily paid compensation to affected persons. The qualifier "voluntarily" suggests the payment to a plaintiff in the context of litigation (including class actions) would be excluded. However, payments made pursuant to a settlement of such actions may well be considered "voluntary." This consideration may become significant in the timing and mechanism of resolving class actions. Note, too, that the language refers to "compensation," but does not specifically require "monetary compensation." "In kind" compensation (such as offers of credit monitoring, etc.) would presumably be included. Finally, any such compensation must be to a person affected "by the violation." It appears that compensation made to settle a negligence or misrepresentation claim pleaded in addition to a breach of privacy claim may not qualify.

Audits: As it can under PIPEDA, under section 96 of the CPPA, the OPC may, on reasonable notice, audit an organization's personal information management practices, if the OPC has reasonable grounds to believe that the organization has contravened the CPPA. Under section 97, after an audit, the OPC must provide the organization with a report of its findings and recommendations. Importantly, this section specifically provides that these audit reports may be included in the OPC's annual report and may therefore become public.

II. The Tribunal

The new Tribunal established under the PIDPTA would also play a significant role in enforcement – and would be a wholly new addition to the privacy enforcement regime. Once the OPC completes its inquiry and finds there to have been a violation of the CPPA, the OPC may recommend to the Tribunal that a penalty be imposed on the organization. The Tribunal would have the following powers and functions:

Imposing penalties: The Tribunal may make an order imposing a penalty on an organization if:

a. The OPC files a copy of a decision in relation to the organizationwith the Tribunal, or the Tribunal, on appeal, substitutes its own decision to recommend that a penalty be imposed.

b. The organization and OPC are given the opportunity to make representations (suggesting some sort of adversarial process and hearing before the Tribunal).

c. The Tribunal determines that imposing the penalty is appropriate.

The financial health of the organization plays a significant role in deciding whether a penalty should be imposed and how much it should be. In determining these issues, the Tribunal must consider: the OPC's analysis, the organization's ability to pay, the effect that paying the penalty will have on the organization's ability to carry on its business, and any financial benefit that the organization obtained from the contravention.

As an added incentive for organizations to develop and implement robust privacy programs, the Tribunal is prohibited from imposing a penalty if the organization establishes that it exercised due diligence to prevent any contravention with the CPPA. The onus here is on the organization to establish the due diligence defence.

Maximum penalties: Under the proposed legislation, the Tribunal's powers to impose penalties are significant. The maximum penalty for all the contraventions in a recommendation taken together is the *higher* of $10,000,000 and 3% of the organization's gross global revenue in the prior financial year. Further, for offences that an organization has knowingly committed, the Tribunal can order fines up to the higher of $25,000,000 and 5% of the organization's gross global revenue in the prior financial year. These penalties are the highest available penalties amongst all countries in the G7.

Hearing of appeals: Under section 100 of the CPPA, both complainants and organizations have a statutory right of appeal to the Tribunal in respect of orders of the OPC. The standard of review for an appeal is *correctness* for questions of law, and *palpable and overriding error* for questions of fact or mixed law and fact.

Decisions of the Tribunal are final and binding, except by judicial review under the Federal Courts Act – it is not subject to appeal or to review by any court. The panel itself will be comprised of three to six appointed members, with only one required to have experience in privacy law.

With respect to procedure before the Tribunal:

- **No technical rules of evidence:** The Tribunal is not bound by rules of evidence (except as concerns privilege), and must deal with all matters as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit.
- **Standard of proof:** In any proceeding before the Tribunal, the standard of proof that a party must discharge is on a balance of probabilities.
- **Majority decision, with reasons:** Decisions will be made by majority, and the Tribunal must provide a decision with reasons in writing to all parties to a proceeding.
- **Public hearings:** Hearings must be held in public. However, the Tribunal may choose to hold all or part of a hearing in private if it believes that

the hearing would not be in the public interest or confidential information may be disclosed. In determining whether the confidential information in issue justifies a private hearing, the Tribunal will consider whether the desirability of ensuring that the information is not publicly disclosed outweighs the desirability of adhering to the principle that hearings be open to the public. This is contrast with the investigations and inquiries portion of the process, during which the OPC is required not to disclose information, subject to certain exceptions. This may well be a factor for organizations in deciding whether or not to drive the OPC to the Tribunal stage.

It is not yet clear how long this process will take, and whether a further jurisdiction review will make the process a lengthy one.

III. Statutory causes of action

The Bill would establish a new private right of action for individuals affected by an organization's CPPA contravention. Under section 106 of the CPPA, an individual affected by an act or omission that constitutes a contravention of the act can sue the organization for damages if the OPC has made a finding under section 92(1) and the finding is not appealed, (b)the Tribunal has dismissed an appeal or the Tribunal has made a finding that the organization has contravened the CPPA. Importantly, this right is not limited to the original complainant, but "anyone affected." This suggests multiple actions would be possible, along with class actions.

CPPA: An in-depth look at the codes of practice and certification program provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

In this article, we address the CPPA's new Codes of Conduct and Certification Program.

A new form of privacy self-regulation

Certification is a way for an organization to demonstrate compliance with legislative requirements. Certification scheme criteria are generally approved by an independent certification body, and may be general or specific. Once an accredited certification body has assessed and approved an organization, it will typically issue an approval or certificate of some sort, relevant to that scheme.

Sections 76 and 77 of the CPPA will bring in new provisions to enable the creation of third-party "codes of practice" and "certification programs" as a means to encourage new sectoral privacy protection self-regulation. The Office of the Privacy Commissioner of Canada (**OPC**) would act as an approval body for entities operating a certification program. The language of the proposed CPPA suggests that participation in these schemes is voluntary (though it is conceivable that licensing bodies could make participation in such a scheme a condition or licensing, or a membership-based organization could make participation a condition of membership).

Organizations may be familiar with this type of self-regulation program as there is a similar concept included in Articles 40 to 43 of the UK and EU General Data Protection Regulations (**GDPR**). GDPR certification must be for a specific processing operation or set of operations that make up a product, process or service offered by an organization. You should decide what product, process or service you offer that you want to have assessed and certified.

What are codes of practice?

If passed, the CPPA would create a framework for entities to create third-party codes of practice and certification programs. An "entity" under sections 76 and 77 of the CPPA includes any type of organization (defined under the CPPA as an association, partnership, person or trade union), and is expanded to include organizations that are not necessarily subject to the CPPA, such as a not-for-profit organization (e.g., Canadian Standards Association (CSA)), affiliations or government institutions.

The entity may apply to the OPC for approval of a code of practice that provides for "substantially the same or greater protection" of personal information as some, or all, of the protections provided for by the CPPA. The language here provides some flexibility so that specific sectors may develop codes of practice that are tailored to the unique aspects of their sector/technologies common in their sector.

For example, an association of insurance providers could develop and submit a code of practice that provides an industry model on how insurance providers shall obtain consent for key data processing activities,

including standard consent language, data sharing around background checks and disclosure of data for the purposes of fraud.

Another example is Canada's banking industry creating an association for the purposes of managing all of the data subject rights under the CPPA. The code of practice could establish a framework to allow banking customers to exercise their rights, including the new data mobility right, requiring one banking institution to transfer a customer's personal information to another banking institution.

A technology-specific code of conduct could be developed by an umbrella organization having a membership focused on the development of artificial intelligence, and developing standards and processes to meet the requirements of algorithmic transparent proposed in the CPPA.

Once developed, the code of practice must be approved by the OPC. This is discretionary, and the OPC "may approve" the code of practice if it determines that the code meets certain criteria, which will be set out in upcoming regulations.

Similar to Article 40 of the GDPR, it is expected that the regulations will require a code of practice to contain mechanisms that will enable mandatory monitoring of compliance of the members to ensure compliance with the code of conduct.

What is the certification program?

An entity may apply to the OPC for approval of a certification program that includes:

- A code of practice;
- Guidelines for interpreting and implementing the code of practice;
- A mechanism to certify compliance with the code of practice;
- A mechanism for the entity to audit compliance with the code of practice;
- Disciplinary measures for non-compliance, including revocation of a certification; and
- Any other requirements that may be provided for by regulation.

Similar to the certification program under the GDPR, it is likely that in order to establish a certification program, entities will be required to enter binding and enforceable commitments via contractual or other legally binding instruments, outlining their obligations to one another, and to data subjects. Further, it is expected that the mechanisms for enforcing compliance and dispute resolution will require an independent body with expertise in privacy law. In the banking example given above, for instance, a mechanism such as an independent body would be in place to resolve disputes around access and mobility.

It is worth noting that under the GDPR, in effect for two and a half years now, no certification scheme has yet been registered.

This type of self-regulation model is not foreign to Canada. AdChoices is the self-regulatory program for online interest-based advertising helping to provide notice, transparency and accountability from the advertising sector online to consumers. The Digital Advertising Alliance of Canada (DAAC) is the not-for-profit consortium of trade associations that is responsible for administering the AdChoices self-regulatory program in Canada.

AdChoices shares many of the components of a certification program: It calls for advertising companies to establish and enforce responsible privacy practices for interest-based advertising aimed to give consumers enhanced transparency and control. Participating companies must adhere to the AdChoices principles, which are enforced by accountability programs, including auditing for non-compliance.

Powers of the OPC

The CPPA would also give the OPC the power to "request" (not require) that an entity operating an approved certification program provide the OPC with information that relates to the program. The scope of this provision is unclear, and could potentially include the OPC requesting information to be used in an investigation of the organization. There is also a provision which empowers the OPC to "cooperate" with a certification entity for the purpose of the exercise of the OPC's powers, duties and function – which clearly contemplates OPC investigations and inquiries. Interestingly, this latter provision is permissive in allowing the OPC to cooperate with entities, but

does not place an onus on the entity to similarly "cooperate" (though this may well find its way into subsequent regulations – see section 122 which permits the Minister of Innovation, Science and Economic Development Canada (ISED) (Minister) to make regulations "respecting record-keeping and reporting obligations of an entity that operates an approved certification program, including obligations to provide reports to the Commissioner in respect of an approved certification program."

Note, too, that the OPC is empowered to disclose information to the Commissioner of Competition that relates to an entity that operations an approved certification program, or an organization that is certified.

The OPC will also have the power to request amendments to the certification program, reject the proposed program and revoke an approval of a certification program in certain circumstances.

Compliance with a certification program is not a "safe harbour"

It is important to note that an organization's compliance with a code of practice or certification program will not relieve an organization of its obligations under the CPPA; nevertheless, there are some benefits.

First, a code of practice and certification program would allow organizations to come together and establish standards of data processing and privacy protections in a manner that is tailored for their industry, their customers, their unique technologies and practices, and their business needs.

Further, a program may mitigate some risk. For example, while the OPC has the power to recommend penalties for contraventions of CPPA, it is prohibited from making such a recommendation "if the Commissioner is of the opinion that, at the time of the contravention...the organization was in compliance with the requirements of an [approved] certification program."

Similarly, while the OPC must investigate complaints, it may decline to do so if the complaint raises an issue in respect of which an approved certification program applies and the organization is certified under that program.

Consequently, a self-regulation certification program can allow an industry to establish its own privacy standards under the CPPA while alleviating the potential costs, resources and overall risk that would be incurred in dealing with the OCP.

However, because compliance with a certification program does not create a safe harbour, it maybe have limited appeal to organizations. If compliance with a certification program requires an assessment as well as a likely fee, whereas compliance with the CPPA can be done internally with limited cost, organizations may not see any benefit in participating in certification programs.

Furthermore, potential certification entities may have reservations about participating. Once an entity and its certification program are approved by the OPC, they are subject to certain aspects of the OPC's powers to which they may not otherwise be subject. For instance, an unincorporated, not for profit industry group that does not handle personal information is likely not subject to PIPEDA. Once it becomes a certificating entity, the OPC has the right to request that it provide certain information, and the Minister may well make regulations pertaining to its obligation to provide reports to the OPC. If that same group still proposed standards and processes for its membership, but did not apply to be a formal certification entity, these provisions of the CPPA would not apply to it.

Will it cost?

The CPPA is silent on the issue of the costs. In other certification schemes, the relevant certification body typically charges a fee to carry out an assessment of processing activity. Cost may vary with the size of the organization and the scale and complexity of the processing operations they are assessing.

Regulations to come

There is much not yet known regarding the details of codes of practice and certification program. The regulations are expected to not only outline the criteria discussed in this article, but the process itself as well, including how to submit an application, the information that must be submitted and when the OCP may revoke its approval of a certification program.

CPPA: An in-depth look at the de-identification provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

This article discusses how the CPPA would treat de-identified information and what it means for businesses.

Background: de-identified information versus anonymized information

De-identified information and anonymized information are generally understood to be different things. De-identified information is information for which the risk of re-identifying the individual is significantly reduced or eliminated in the context in which it is to be used. This generally includes removing or obscuring both "direct identifiers" (i.e. attributes that alone enable unique identification of an individual) and "indirect identifiers" (i.e. attributes that, when combined with other information, enable identification of an individual). De-identified data can necessarily be "re-identified." The method for doing so depends on the particular de-identification technique. For example, where data is de-identified by replacing identifying information with random codes (i.e. "pseudonymization"), there would generally be a separately stored key that could be applied to the codes to restore the identifying information. In other words, de-identified information can be re-identified, with varying degrees of difficulty.

Anonymized information is information which cannot be re-identified in any context. Because of that, it generally falls outside the reach of privacy laws. In order to be truly anonymized, an organization must strip personal information of a sufficient number of elements such that the individual can no longer be identified. However, if it is possible to use any reasonably available means to re-identify the individuals to which the information refers, that data will not have been effectively anonymized but will have merely been de-identified. A failure to understand this distinction means that organizations that believe they have "anonymized" data may, in fact, be handling "de-identified" data and are therefore still subject to privacy laws.

How does PIPEDA treat de-identified information?

PIPEDA is silent on the collection, use or disclosure of de-identified information. The question of where to draw the line between identifiable and anonymous information has thus far been left to the Office of the Privacy Commissioner (**OPC**) and the courts. The OPC stated in its 2013 Information Bulletin: Personal Information that personal information that has been de-identified does not constitute anonymous information (and is thus personal information for the purposes of PIPEDA) if there is a serious possibility that someone could link the de-identified data back to an identifiable individual (see also PIPEDA Case Summary #2009-018). This statement from the OPC builds on the decision in *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII), which looked at the definition of "personal information" pursuant to an access request made under a related statute, the *Access to Information Act*.

The OPC has also stated that information is only "truly" anonymous (and hence not "personal") when it can never be linked to an individual, either directly or indirectly. This threshold is higher than in some other

jurisdictions, such as the UK. In the UK, the High Court in *R (on the application of the Department of Health) v Information Commissioner* [2011] EWHC 1430 (Admin) stated that the risk of identification must be greater than remote and reasonably likely for information to be classed as personal data under that country's privacy law.

How do other jurisdictions treat de-identified information?

In the years since PIPEDA became law, data-driven technologies have become significant drivers for innovation, economic growth, and socially beneficial purposes in both the public and private sectors. The value of the data that powers many of these technologies can often be realized without the inclusion of personal information. Recognizing this, jurisdictions around the world have sought to address the use of de-identified data in their regulatory regimes.

The EU's GDPR provides that pseudonymized data, while still "personal," may be used for purposes other than those for which it was collected. In addition, data controllers may use pseudonymization to satisfy GDPR's data security requirements, and in some circumstances controllers need not satisfy certain data subject requests related to pseudonymized data. In other words, while pseudonymized data is still caught by the GDPR, it takes a more flexible approach to such data. Recital 26 of the GDPR states that the legislation is not concerned with the processing of anonymous information.

California's CCPA excludes de-identified information from its reach entirely, provided that the controlling business implements safeguards and processes prohibiting re-identification, as well as processes to prevent the inadvertent release of de-identified data, and does not make any attempt to re-identify the information.

Under both GDPR and the CCPA, data is considered de-identified when it is not reasonably likely that it could be used to re-identify the individual.

How would the CPPA define de-identified information?

If passed, the CPPA would not actually define "de-identified information." Instead, it would define the process of de-identification: "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."

The CPPA would thus bring de-identified information squarely within the scope of Canada's federal private sector privacy regime.

The inclusion of de-identified information under CPPA would be broadly consistent with the OPC's prior commentary that de-identified information may still be "personal." Essentially, the CPPA would carve out "de-identified" information as a subset of "personal information" to which certain exemptions or obligations would apply. This is similar to how de-identified information is treated under the GDPR, but falls short of a total exclusion as is the case under the CCPA.

In addition, the CPPA would shift the line between "de-identified" and truly anonymous information. Information would be "de-identified" (and hence not anonymous) where re-identification is "reasonably foreseeable," rather than a "serious possibility." In theory, this would broaden the scope of what would be considered "de-identified" information (and thus regulated), and narrow the scope of what would be considered anonymous information (and thus not regulated). This would also bring Canada into line with the international regulations described above.

As currently drafted, the CPPA does not provide any further detail as to when re-identification would be "reasonably foreseeable." Rather, the CPPA would require organizations to ensure that any technical or 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.

At a minimum, it seems that organizations would be expected to balance the method of de-identification against the proposed use of the de-identified information, as well as the information's sensitivity.

The inclusion of the "purpose" and "sensitivity" considerations is a bit confusing. It appears that what is intended here is that the more robust de-identification measures should be used where the personal information is particularly sensitive, and the purpose exposes the de-identified information to increase risk (for instance, used for a public facing purpose as opposed to being limited to internal use only). This is really a risk of harm analysis, and may be more understandable framed that way: are the measures applied proportionate to the harms that could result if the information were to be re-identified?

Organizations would not be required to use a particular technique of de-identification, as is the case under the GDPR (i.e. pseudonymization), and could seemingly use methods such as randomization (i.e. modifying data attributes such that their new value differs from their true value in a random way) or aggregation (i.e. grouping values into ranges).

What about information created from personal information?

The definition in the CPPA specifically captures "information create[d] from personal information." This is very broad, and creates the potential for overreach, in which very little information can ever be anonymous (and therefore escape privacy laws).

For example, if a company were to take a list of mailing addresses of its customers and from that, generate a list of sales volumes by the first three digits of postal code alone, this list appears to be captured under the CPPA as "de-identified" information (based solely on the fact that it was created from personal information). In fact, the way the language is drafted, it is impossible for any information derived from personal information to ever be anonymous simply because it is derived from personal information. The most it will ever be is de-identified.

Under the current PIPEDA, it is likely the list would simply not be personal information, and not subject to regulation (e.g., safeguarding, general use without consent, etc.).

Note, too, the disposal requirements of the CPPA, which we address in a separate article in this series. Disposal is the "permanent and irreversible deletion" of personal information. Unlike in PIPEDA, there is no provision for anonymization qualifying as disposal. As a result, absent any grandfathering of existing data sets, organizations that have relied on anonymization as a form of destruction will need to update their policies and procedures to ensure "permanent and irreversible" deletion. If grandfathering is to be permitted, then organizations may wish to anonymize critical data sets prior to the coming into the force of the CPPA, as after that date, these data sets would only be de-identified information still subject to the CPPA, with no avenue to remove it from the CPPA's purview.

What would an organization's obligations be with respect to de-identified information?

Organizations would be prohibited from re-identifying an individual from de-identified information (alone or in combination with other information), except in order to conduct testing of the effectiveness of any security safeguards. Note that the "combination" that is contemplated here is not just with other personal information, but with any other type of information.

In addition, organizations contemplating a prospective business transaction must now de-identify any personal information before using it or disclosing that context (more on business transactions below).

What would organizations be able to do with de-identified information?

Organizations would be able to de-identify an individual's personal information without their knowledge or consent. Organizations would then be able to use or disclose such de-identified information without the knowledge and consent of the individual in the following circumstances:

- Organizations would be able to use de-identified information for their own internal research and development purposes.
- Parties to a prospective business transaction would be able to use and disclose de-identified information in order to assess and complete the transaction, provided the information would remain de-identified until they completed the transaction. This provision would essentially make the existing business transaction exemption under PIPEDA more exacting by requiring information to be de-identified. Note that there would no longer be a

provision that allows actual personal information to be used or disclosed by the parties to a prospective business transaction (as there currently is in PIPEDA). The information must be de-identified.

- Organizations would be able to disclose de-identified information for a socially beneficial purpose to specific entities, including:
    - a government institution or part of a government institution;
    - a health care institution, post-secondary educational institution or public library in Canada;
    - any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution, to carry out a socially beneficial purpose; or
    - any other prescribed entity.

A "socially beneficial purpose" would be defined 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."

CPPA: An in-depth look at the data mobility provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

This article addresses the CPPA's proposed introduction of a data mobility right that would allow individuals to request that their personal information be shared between organizations, subject to certain limitations and qualifications.

The CPPA recognizes the concept of "data mobility"

PIPEDA does not recognize or address the concept of "data mobility," which Innovation, Science and Economic Development Canada (the government) defined in its 2019 *Proposals to modernize the Personal Information Protection and Electronic Documents Act* paper (the **PIPEDA Modernization Paper**) as "enabling individuals to request that the personal information that they have provided to an organization, be provided to another organization."

To address this gap, the CPPA explicitly references a right of mobility of personal information. Proposed section 72 states:

> Subject to the regulations, on the request of an individual, an organization must as soon as feasible disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework provided under the regulations.

Why is data mobility important?

In theory, data mobility allows individuals to better and more easily control who has access to their information. When a framework for data mobility is in place, individuals are able to direct the movement and sharing of their information between organizations in a lawful and trusted way.

Absent such a framework, this type of data sharing can be fraught with risks, both for the organization sharing the data (for example, the reputational risk that comes with sharing personal information with another organization in a manner that could harm an individual) and the individual wishing to have that personal information shared (who may have their personal data misused or shared in a manner that otherwise harms them). Bi-lateral agreements between the transferring organization and the receiving organization can mitigate some risk via appropriate contractual terms, however bi-lateral agreements only allow the individual to request their information be provided to an organization chosen by the transferor, not by the individual.

A well-articulated framework can help mitigate these risks and create certainty for organizations that share personal information, and allow greater choice for individuals. According to the government, this certainty in turn helps foster innovation by providing transparent and consistent rules for organizations to adhere to when developing new products that leverage personal information. As the government noted in its PIPEDA Modernization Paper:

> Studies in other jurisdictions have determined that data mobility has the potential to enhance consumer choice thus fostering the emergence

and growth of innovative new goods and services, in addition to supporting greater individual control over data and encouraging competition.

From reading section 72 above, it is clear that it is simply the first step (albeit an important one) in the establishment of a data mobility framework for Canadians. Even though enabling regulations are not yet available, some key elements of data mobility under the CPPA are clear.

The individual directs the sharing

Under the CPPA, data sharing would be initiated at the request of the individual, not the organization sharing the data. A core concept of data mobility is individual empowerment, allowing individuals to direct and control the ways in which their data is shared.

Personal information must be shared as soon as feasible

The disclosure of information must be "as soon as feasible" – speed is important in the digital world. A data-sharing framework that allowed an organization to delay that sharing would render the framework ineffective.

However, there are some elementary considerations that will influence "as soon as feasible." For instance, there needs to be agreement on how the information is to be shared (e.g., API? Excel spreadsheet?) and in what format – and organizations must have the technical compatibility to do so. These elements will presumably be addressed by the data mobility framework.

Participation in the data mobility framework

An organization can only share data with another participant in the framework. If an individual wishes to port their data to an organization that operates outside the framework, the protections and standards afforded by the regulations will not apply (however, it does not appear that individuals will be prohibited from sharing their personal information from non-participating organizations; it is just that they will have to do it themselves instead of via direct transfer from organization to organization).

Participation in any data mobility framework will likely be contingent upon the organization's adoption of and adherence to certain security standards, requirements for format, specifications for transfer mechanisms, and so on. It is also probable that the "data mobility framework" will not be a single framework, but a series of sector-specific frameworks rolled out over time. This was the approach taken in Australia, with its equivalent consumer data right.

Scope of information subject to the mobility right

The language of section 72 of the proposed CPPA suggests that the right encompasses "personal information [the organization] has collected from the individual." This is a fairly narrow scope of information and suggests that information the organization has collected from third parties (e.g., a credit score) or that it itself generates about an individual (e.g. identity verification or a customer preferences profile) would not be subject to this right.

Interestingly, the emphasis here on "collection" is in contrast with the notion of an accountable organization, which would change under the CPPA. Under PIPEDA, the organization accountable for personal information was the one that collected the personal information. Under the CPPA, the accountable organization would be the one "that decides to collect [the personal information] and that determines the purposes for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization."

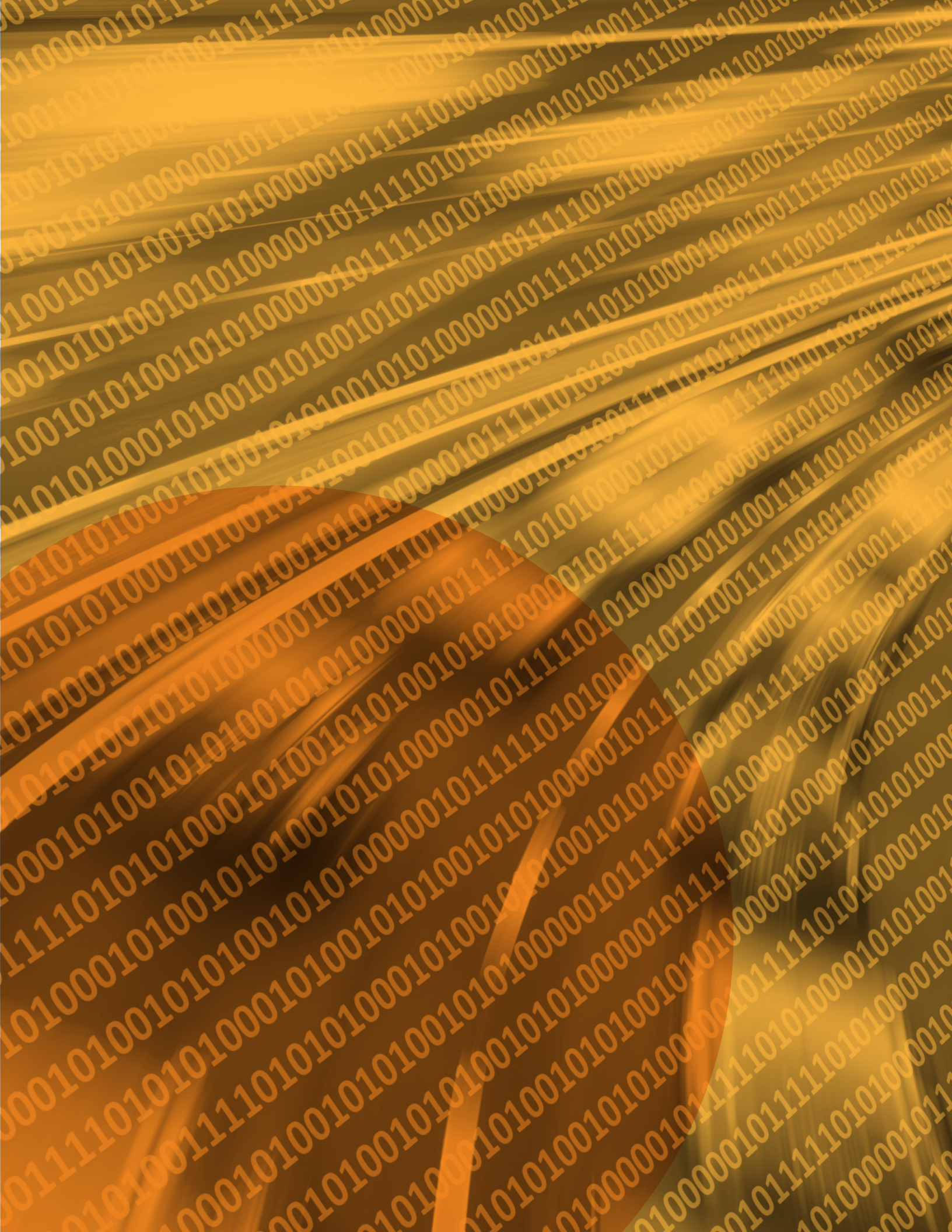
For some business models, there is potential here for a disconnect. For instance, for a business in which a central organization has multiple other entities, the entities may be the actual collectors of the information from the individual, which they then provide to the central organization, and it is the central organization which is the one making decisions about the collection, use and disclosure of that information. In this scenario, the mobility right appears to apply to the entities, because they "collect" the personal information from the individual, even though it is the central organization which is the accountable organization. If this is true, organizations (and affiliated entities) will need to think about how the data mobility right might apply to them, and how they are going to manage it.

In addition, implicit in section 72 is the idea that an organization has a repository of personal information on each individual that is easily identified, organized

and shared. It is likely that most Canadian organizations have never maintained data in this manner. Separating personal information from all other corporate information an organization maintains on an individual could be technically difficult and so costly that it acts as a barrier to entry into the framework. Since the framework can be thought of as enabling a network of interconnected organizations, it would benefit from a network effect, with the value of the framework increasing as more organizations sign on to it. Providing tools and resources for organizations to organize and store their personal information in a manner that allows them to securely share it in a compliant manner could help determine the overall success of data mobility rights in Canada. Industry organizations, interest groups, and even the government itself may wish to consider this.

What are the next steps?

Like so many legislative proposals, when it comes to data mobility, the devil is truly in the details. Bill C-11 references a "data mobility framework" to be provided for under the regulations. However, at this early stage, draft regulations have yet to be proposed. Until they are, section 72 puts a stake in the ground, signaling that the government believes data mobility is a key piece in moving privacy regulation firmly into the digital age.



CPPA: An in-depth look at the disposal provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

This article addresses the CPPA's new requirement to dispose of personal information when that information is no longer required, or upon request to do so.

Expanded obligations to dispose of personal information

There is no explicit requirement in PIPEDA to delete or destroy personal information. Principle 5 (in Schedule 1 to PIPEDA).

PIPEDA does impose limits on the retention of personal information. For instance, organizations are required to retain personal information "that has been used to make a decision about an individual … long enough to allow the individual access to the information after the decision has been made. In addition, PIPEDA says that "[p]ersonal information shall be retained only as long as necessary for the fulfilment of [the purposes for which it was collected]."

Principle 5 does state that organizations "should" destroy, delete or anonymize personal information that is no longer necessary to fulfil the purposes for which it was collected, but does not go so far as to make destruction a clear obligation.

The approach taken by the CPPA would solidify these existing principles into an obligation, and add a further obligation to dispose of personal information on request.

Personal information must be disposed of after its lifecycle

Section 53 of the CPPA addresses the disposal of personal information at the end of its lifecycle. It expressly prohibits retaining personal information for any period of time beyond what is necessary to "fulfil the purposes for which the information was collected, used or disclosed" or otherwise comply with legal requirements including "reasonable" contract terms. It also clearly requires organizations to dispose of personal information "as soon as feasible" after the end of that time period.

As under PIPEDA, section 54 of the CPPA would require organizations to retain personal information used to make a decision about an individual "for a sufficient period of time to permit the individual to make a request for access". There is no information on what length of time is considered "sufficient" but typically is at least as long as required to exhaust all avenues of appeal or review.

Personal information must be disposed of on request

The more substantial change is that, pursuant to section 55 of the CPPA, organizations would be required to dispose of an individual's personal information if the individual requests it. There is no time limit on this request and so information currently being used for an identified purpose can be the subject of a disposal request.

The only exceptions to the obligation to dispose of information on request are where another individual's personal information is not severable and would also be disposed of, or where other requirements under federal or provincial law or "reasonable" contract terms prevent the organization from disposing of information. Where

an organization refuses a request for disposal, it must inform the individual in writing, provide reasons for the refusal, and explain the further steps that the individual can take.

The severability exemption will be of note to organizations using aggregate data sets or training machine learning algorithms, as this type of data is unlikely to be severable in any commercially reasonable way. With respect to the disposal exemption for "reasonable" contract terms, organizations would be well advised to consider reviewing existing terms for such reasonableness if they anticipate potentially relying on them to refuse disposal requests. See more on this point below.

Managing disposal requirements

From a procedural perspective, this new obligation to dispose of personal information on request will require organizations to bring together the policies and procedures that allowed them to respond to requests for disclosure or correction of personal information with the policies and procedures for disposal of information at the end of its lifecycle.

In particular, organizations will need to track two points in time: the time after which personal information is no longer needed for its purposes, as well as the last time personal information was used to make a decision about an individual. Organizations will also need to set procedures to ensure that the personal information is disposed of "as soon as feasible" after the later of those two points in time, and ensure documentation of it.

Although these requirements do impose a new burden on organizations, they also reduce the risk when a data breach occurs. When an organization does not dispose of personal information that is at the end of its lifecycle, it also effectively creates a larger trove of personal information for potential loss or theft. Conversely, regular disposal of personal information limits what can be taken in the case of a breach.

Anonymization is not disposal

PIPEDA permitted organizations to erase, destroy or anonymize personal information at the end of its lifecycle. The CPPA, however, appears to preclude anonymization as a means of disposal.

Under the CPPA, the "disposal" of personal information is defined as "the permanent and irreversible deletion of personal information". There is no provision for anonymization, as there is in PIPEDA.

The CPPA does permit the "de-identification" of personal information, but this does not qualify as disposal. Because the definition of de-identification includes the "creat[ion] of information from personal information", the anonymization of personal information can only ever create de-identified information, which is still subject to the CPPA, and still subject to disposal requirements.

General issues surrounding anonymized versus "de-identified" information are discussed in a separate article.

Given the high threshold for disposal ("permanent and irreversible deletion") and the ever-changing nature of technology, organizations will need to regularly review their policies and procedures to ensure that their deletion strategies are effective. Further, absent any grandfathering of existing data sets, organizations that have relied until now on anonymization as a form of destruction will need to update their policies and procedures to ensure "permanent and irreversible" deletion. If grandfathering is to be permitted, then organizations may wish to anonymize critical data sets prior to the coming into the force of the CPPA, as after that date, these data sets would only be de-identified information, which is still subject to the CPPA, with no avenue to remove it from the CPPA's purview.

As noted, the CPPA appears to continue to view "de-identified" personal information as personal information. As a result, the disposal provisions would also apply to de-identified personal information. This could create substantial risk for organizations relying on de-identified personal information.

What are "reasonable" contract terms?

The CPPA adds a further new wrinkle to the disposal requirements: an organization need not dispose of information if "reasonable" contract terms prohibit its disposal. This exception applies to both the obligation to dispose of personal information at the end of its lifecycle and the obligation to dispose on request.

Because it is new, it is not clear from the current wording of the CPPA what contractual terms will be

"reasonable" and provide the basis for the exception. Some inferences can nonetheless be drawn from the proposed legislation as a whole.

Section 5 of the CPPA sets out the overarching purpose of the act: to balance "the right of privacy of individuals with respect to their personal information" and "the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." To be reasonable, contract terms should therefore also seek to balance these two factors. Organizations should also consider limiting the contract terms to situations that "a reasonable person would consider appropriate in the circumstances."

Impacts on privacy policies

The CPPA includes some substantial changes to the requirements for privacy policies, which are discussed in a separate article. In relation to the right to request disposal, organizations must include information in their privacy policies regarding how individuals can make that request. This information must be "readily available" and be written in "plain language."

Disposal requirements for service providers

The changes in service providers' obligations generally under the CPPA are discussed in a separate article.

Under section 55(3) of the CPPA, an organization that receives a request for disposal must, in addition to disposing of the personal information in its possession, inform any service provider of the request and ensure that the service provider also disposes of the personal information.

It is implicit in this term that organizations will have a record of what and whose personal information they have transferred to service providers. Organizations that do not already track this will therefore be required to perform and update data mapping.

Section 55(3) implies that service providers will dispose of the personal information, but does not expressly require them to do so. Instead, it leaves the obligation on the organization which received the request to "obtain a confirmation from the service provider that the information has been disposed of."

As a result, it would be prudent for organizations using service providers to include contract terms requiring the service providers to track disposal requests and dispose of personal information promptly and in accordance with the CPPA. Such terms may also assist with the due diligence defense to an administrative monetary penalty, which will be discussed further below.

Is this the "right to be forgotten"?

The likely impetus for the new disposal requirements in the CPPA is the "right to be forgotten" that has developed in the European Union and is now set out in s. 17 of the GDPR. As Innovation, Science and Economic Development Canada put it in their Fact Sheet on the CPPA:

> Disposal of personal information and withdrawal of consent: The accessibility of information online makes it hard for individuals to control their online identity. The legislation would allow individuals to request that organizations dispose of personal information and, in most cases, permit individuals to withdraw consent for the use of their information.

This is similar reasoning to that underpinning the right to be forgotten.

However, the disposal requirements in the CPPA remain much narrower than the EU's "right to be forgotten". In particular, there is no mention in the CPPA of de-indexing from search engines. Given the ongoing reference by the Privacy Commissioner of Canada to the Federal Court on that issue, the exclusion is likely deliberate. The obligations are instead limited to deletion of personal information by an organization that has collected the information.

The decision to limit deletion in this way in the CPPA is also different from the approach currently being taken in Québec. Its Bill 64, which sets out substantial amendments to the current Québec privacy legislation, explicitly adds a right to de-indexing (section 28.1).

The consequences of failure to dispose of personal information are serious

The CPPA generally sets much higher administrative monetary penalties, or fines, than PIPEDA. Another article covers new penalty and enforcement provisions in detail.

For the purpose of this article, the key point is that an organization that does not dispose of information at the end of its lifecycle, under section 53, or after a request under section 55, may be subject to administrative monetary penalties of up to the higher of $10 million and 3% of its gross global revenue in the previous financial year.

However, this administrative monetary penalty cannot be imposed if the organization "establishes that it exercised due diligence to prevent the contravention" (section 94(3)). The due diligence defence is yet another reason for organizations to have robust privacy policies and practices.

CPPA: An in-depth look at the consent provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

This article addresses the CPPA's new consent requirements and new exemptions from having to obtain consent.

The basics of consent

Consent is a key element of PIPEDA, and would continue to underpin the CPPA. Under PIPEDA, organizations are required to obtain meaningful consent for the collection, use and disclosure of personal information. Consent is considered meaningful when individuals are provided with clear information explaining what organizations are doing with their information.

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations must take into account the sensitivity of the information – more sensitive information will require express consent; less sensitive information can be used with opt-out consent. In obtaining consent, the reasonable expectations of the individual are also relevant.

Very little of this would change under the CPPA. However, in recognition of the challenges posed by data-intensive business models, and consumer difficulty understanding privacy policies, consent under the CPPA has been re-worked and would, among other things, create exemptions from having to obtain consent for certain well understood and common business activity uses, and require express consent for all collection, use and disclosure unless an organization could demonstrate that opt-out (or implied) consent was appropriate.

Appropriate purpose, reasonableness would need to be documented

Under PIPEDA, even with consent, an organization may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. Often, businesses interpret this requirement to mean what is reasonable to them and their commercial interests; this is not a correct understanding of this requirement.

The CPPA attempts to provide clarity by adding in new "factors" that must be considered when trying to determine whether a purpose is reasonable (section 12):

a. the sensitivity of the personal information;

b. whether the purposes represent legitimate business needs of the organization;

c. the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;

d. whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and

e. 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.

These factors derive from the "reasonableness test" established by the Federal Court in the *Turner v. Telus Communications Inc.* case (subsequently affirmed by Federal Court of Appeal), which set out factors for evaluating whether an organization's purpose was in compliance with subsection 5(3).

Note that consideration of these factors is mandatory ("must"). A failure to do so would be a violation of the CPPA. Organizations may want to document that they have considered the factors of the reasonableness test that would be newly required under the CPPA.

Detailed, plain language consent would be required

The CPPA formalizes what were Principles in PIPEDA, supplemented by OPC guidance, and adds additional specific requirements. Under PIPEDA, consent was valid only if was reasonable to expect the individual at whom the organization's activities were directed would understand the nature, purpose, and consequences of the of the collection, use or disclosure.

The CPPA would remove the interpretative ambiguity be prescribing (section 15(3)) certain elements that would by required to be disclosed. This information would have to be provided at or before the point at which the organization seeks the individual's consent. In addition, this information must be provided in plain language. The elements which must be disclosed are:

a. the purposes for the collection, use or disclosure of the personal information determined by the organization and recorded under subsection 12(3) or (4);

b. the way in which the personal information is to be collected, used or disclosed;

c. any reasonably foreseeable consequences of the collection, use or disclosure of the personal information;

d. the specific type of personal information that is to be collected, used or disclosed; and

e. the names of any third parties or types of third parties to which the organization may disclose the personal information.

This has obvious implications for organizations, many of which will need to rewrite and redesign privacy policies. Online processes may need to re-designed to ensure that consumers have this information available "at or before" the point at which consent is sought.

Prohibition on "tied selling" expanded

Under PIPEDA, an organization is prohibited from, as a condition of the supply of a product or service, requiring an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil "the explicitly specified, and legitimate purposes."

The CPPA removes the "legitimate purposes" justification for collection, use, or disclosure of personal information without consent. The new threshold under the CPPA would be whether personal information is "necessary to provide the product or service", as opposed to the broader, and potentially more flexible threshold of what constitutes a "legitimate purpose". From a compliance perspective, organizations will likely need to review their collection and use of personal information to determine if it is necessary, and document this.

Business contact information exemption narrower

PIPEDA creates an exemption for business contact information, defined to include "any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession."

The CPPA would narrow this, and now provides an exemption only for (emphasis added) "personal information that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession".

Consent obtained by providing false or misleading information invalid

Furthermore, the CPPA would contain an express provision (section 16) stating that any consent obtained by providing false or misleading information or using deceptive or misleading practices would not be valid. This dovetails with the "false or misleading representations" in the *Competition Act*, and creates double the risk for organizations which fail to get this right.

Businesses should review their privacy policies and consent documentation against current business activities to ensure they are not obtaining consent by deception.

Exemptions from withdrawal of consent narrowed

Under PIPEDA, individuals have a right to withdraw their consent at any time, "subject to legal or contractual restrictions and reasonable notice." Under the CPPA, these exemptions would be narrowed by more specific language: "subject to this Act, to federal or provincial law or to the reasonable terms of a contract".

The CPPA also expressly permits the withdrawal of consent "in whole or in part" in section 17(1). Partial withdrawal of consent (e.g., for some activities, but not others) is not specifically contemplated in PIPEDA.

Collection and use without knowledge or consent expanded

Many of these exemptions exist under PIPEDA. However, a significant change in the CPPA would see organizations no longer needing to seek consent for certain defined, well understood business purposes (section 18(1)), as well as certain uses of de-identified information.

Under the CPPA, knowledge and consent would not be required for:

1. *Business activities (which don't include certain marketing activities)*

For instance, the CPPA would allow organizations to collect or use (but not disclose) an individual's personal information without their knowledge or consent if the collection or use is made for a listed business activity (described further below) and:

a. a reasonable person would expect such a collection or use for that activity; and

b. the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

Importantly, not all business activities qualify. Only the following activities, listed in section 18(2), would qualify:

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.

It is worth noting that by virtue of the provision in section 18(1)(b) above, collection or use related to targeted advertising, or delivering "nudges" or recommendations would likely be excluded from this provision, and consent, would therefore be required. Under the CPPA, section 15(4), such consent would need to be express – unless the organization can establish "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 that is to be collected, used or disclosed." The exclusion of these types of marketing activities from the ambit of this exemption will likely be of concern to many organizations, particular y those that provide or use ad tech.

Under the CPPA, organizations will also need to be mindful that they and their employees don't make the assumption that because the personal information is being used for one of the enumerated activities, it must be okay to use if for other activities, which are not enumerated. If this were to occur, there is a significant risk those "other" activities would be using the personal information without adequate consent, without the benefit of falling within the exempted activities.

2. *Transfers to service providers*

Under the CPPA, transfers to a service provider would not require knowledge or consent, stating explicitly what was largely already found in OPC guidance.

Because of this, however, it is important that organizations acting as service providers be very careful about how the scope of their processing activities is defined in their service contracts with

accountable organizations. If a service provider strays outside the permitted processing (e.g., aggregation, drawing statistical inferences, market insights, etc.), it will no longer benefit from being excepted from many of the CPPA provisions, and will itself become the accountable organization – and likely be unable to demonstrate it has appropriate consent for the out-of-scope processing.

3. *De-identification, and certain uses of such information*

An organization does not require an individual's knowledge or consent to de-identify personal information. However, de-identification does not give an organization carte blanche to use it in any way it sees fit. De-identified information remains under the purview of the CPPA and can only be used in the following ways:

- for internal research and development purposes (section 21);
- for prospective business transactions (section 22(1)) and completed business transactions (section 22(2)) (where "business transaction" refers to, among other things, the purchase, sale or other acquisition or disposition of an organization); and
- for disclosure to a prescribed entity, but only if it is for a "socially beneficial purpose" (section 39).

Note that the requirement that information be de-identified prior to being disclosed for a prospective or completed business transaction is new. Under PIPEDA, the disclosure of personal information itself was exempted; this would no longer be the case. Organizations should be aware that, under the CPPA, where de-identification of relevant information is not possible, or not appropriate, consent will be required. Provisions to this effect should be contained within a privacy policy to ensure organizations aren't hamstrung by this requirement at the time of the business transaction.

CPPA: An in-depth look at the access request provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

This article discusses how the CPPA would treat requests made to organizations by individuals seeking to access their personal information.

Background: the right of access under PIPEDA

Under PIPEDA, individuals have the right to access and correct personal information about them in the custody or control of an organization subject to PIPEDA. This right of access is governed by Principle 9 of Schedule 1 to PIPEDA. Under the CPPA, the right of access would be incorporated into the legislation itself. The mechanisms for submitting and responding to an access request, as well as available exemptions, would also be included in the legislation itself. As in PIPEDA, the CPPA would require such requests be made in writing, and organizations would be required to provide access to the information requested unless the organization can provide justification for acting otherwise, or such access is prohibited.

The right of access

The right of access under the CPPA would be largely the same as that under PIPEDA. Upon the written request of an individual, an organization would be required inform the individual of whether it has personal information about the individual, how it uses that personal information, and whether it has disclosed that personal information (section 63(1)). The organization would also need to provide the names of the third parties, or the types of third parties, to which it has disclosed personal information (section 63(2)). Note that the language here is in the alternative – organizations that do not want to provide the names of third parties to which have disclosed an individual's personal information can still satisfy this requirement by providing a description of the type of organization to which they provided the information.

New under the CPPA would be an access right specific to automated decision making. Under the CPPA, if an organization has used an "automated decision system" to make a "prediction, recommendation or decision about the individual," and an individual makes a request, the organization would need to provide the individual with an explanation of the prediction, recommendation or decision, and an account of how the personal information used to make the prediction, recommendation or decision was obtained.

All of the above must be provided in "plain language."

The access right in respect of automated decision systems is likely to cause the most concern. Given the breadth of the definition ("any technology that assists or replaces the judgement of human decision-makers"), it is likely that organizations will be unclear on what is or is not captured, and therefore to what requests for information they must provide an explanation and how the personal information was obtained for it.

Where requested, an organization would also be required to give the individual access to their information. As with PIPEDA, the CPPA would not require organizations to actually provide a copy of this information; in practice, however, most organizations do provide copies, at least for easily accessible, electronic copies.

Thirty-day response time remains

There would be no changes to timelines under the CPPA. An organization would be required to respond to an access request within thirty days of receiving it. In certain circumstances, an organization would be entitled to extend the thirty-day time limit by sending a notice of extension to the individual within thirty days, setting out a new time limit and informing the individual of their right to make a complaint to the Office of the Privacy Commissioner of Canada (**OPC**). An organization would only be entitled to extend the time limit where:

- Meeting the access request within the initial thirty-day time period would unreasonably interfere with the organization's activities, or if the organization would require more time to undertake consultations necessary to respond to the request. In these circumstances, the organization would be entitled to extend the time limit by an additional thirty days.
- An organization requires additional time to convert the personal information into an alternative format (i.e., a format allowing an individual with a sensory disability to read or listen to the personal information).

As discussed below, organizations would be entitled to refuse access requests in certain circumstances. In these cases, organizations would be required to provide reasons for the refusal, and set out the individual's recourse to make a complaint to the organization or to the OPC.

Charging a fee is permitted, but fee must be minimal

An organization would be prohibited from responding to the individual's request at a cost unless the organization had informed the individual of the approximate cost of responding to the request, the cost to the individual would be minimal, and the individual had advised the organization that the request was not being withdrawn.

Mandatory and discretionary exemptions to the right of access

Unlike PIPEDA, the CPPA would more clearly define the circumstances under which an organization would be able to refuse an individual's access request.

In certain cases, access is prohibited. An organization must refuse access if granting the request would "likely reveal personal information about another individual." However, if the information about the other individual were severable from the information about the requester, the organization would be required to sever the information about the other individual and grant access to the remainder.

Note that under the CPPA, the severed information may qualify as having been de-identified under the CPPA's definition of "de-identify". As a result, the organization must, pursuant to section 74, "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." See our article on de-identification in this series.

Severance is likely to be straightforward where information appears in forms or emails or other structured formats. Blended information (e.g., aggregate data sets) poses more of a challenge and will in most cases be unable to be severed.

Refusal of requests continues to be permitted in narrow circumstances

Organizations would have the discretion to refuse access to information where:

a. The information was protect by solicitor-client or litigation privilege;

b. Granting access would reveal confidential commercial information;

c. Granting access could reasonably be expected to threaten the life or security of another individual;

d. The information was collected pursuant to the exception to knowledge and consent for the purposes of an investigation under s. 40(1) (in other words, where personal information was collected without the knowledge or consent of the individual for purposes related to investigating a breach of an agreement or a contravention of federal or provincial law. Organizations relying on this exemption must notify the OPC of this);

e. The information was generated in the course of a formal dispute resolution process; or

f. The information was created for the purpose of making a disclosure under the Public Servants Disclosure Protection Act or in the course of an investigation into a disclosure under that Act.

In the circumstances described at (b) and (c), the organization would be required to sever the information giving rise to the discretionary exemption and provide access to the remainder.

If the individual needed the information requested because an individual's life, health, or security was threatened, none of the above exemptions would apply and organizations would be required to provide access to the information. Note, however, that the prohibition against disclosing the personal information of other individuals continues to apply in these circumstances.

Access to information subject to certain exceptions

Like PIPEDA, the CPPA would enable organization to disclose personal information to a government institution or part of a government institution without the knowledge or consent of the individual for the purposes of law enforcement, national security, defence, international affairs, or complying with a subpoena, warrant, or order.

Where an individual had made an access request for such information or for an account of such disclosures, the organization would have to notify the institution of the request. The institution would then be entitled to object to the organization's compliance with the request on the basis that compliance would be deleterious to:

- National security, the defence of Canada or the conduct of international affairs;
- The detection, prevention or deterrence of money laundering or the financing of terrorist activities; or
- The enforcement of a federal or provincial law or law of a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

The organization would then be required to refuse the request and notify the OPC, and would be prohibited from disclosing to the requester the fact that the organization had notified the government institution.

The right to amendment

As with PIPEDA, if an individual given access to their personal information is able to demonstrate that the information is not "accurate, up-to-date or complete", the organization would be required to amend the information as required. After doing so, the organization would be required to transmit the amended information to any third party with access to it.

In the event that the organization and individual could not agree on the amendments, the organization would be required to record the disagreement, and if appropriate to do so, inform parties with access to the information that there was a disagreement.

Right to complain continues under the CPPA

An individual unhappy with the outcome of their request may complain to the organization itself, which is required under section 73(3) to investigate such complaint and "make any necessary changes to its policies, practices and procedures as a result of the investigation."

CPPA: An in-depth look at the private right of action

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

When does a private right of action arise under the CPPA?

The CPPA will contribute to Canada's burgeoning privacy jurisprudence by introducing a private right of action for individuals affected by an organization's conduct that is found to be in breach of the statute. The private right of action would allow individuals to seek financial relief from the court for various violations of the CPPA, if the Office of the Privacy Commissioner of Canada has first made a finding that the organization has contravened a provision of the CPPA.

Under PIPEDA, no such right currently exists. However, under section 14(1) of PIPEDA, a complainant may, after receiving the Commissioner's report (or being notified by the OPC that the investigation of the complaint has been discontinued), apply to the Federal Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, provided the matter is referred to in the list of clauses that are enumerated. The Court may make an order and/or award damages to the complainant, including damages for any humiliation that the complainant has suffered. Damages awarded to individuals under this provision have typically been nominal. However, class actions may be possible under this section, and can make even nominal damages awards significant in the aggregate.

How can a claim be brought?

There are two ways in which an individual would be able to bring a civil claim under the CPPA. The first is set out in section 106(1), which grants an individual a private right of action for damages for loss or injury that an individual has suffered as a result of an organization's contravention of the CPPA. The individual must be "affected by" the act or omission of the organization which means the right is not limited to the complainant in an inquiry. For example, a class action could be commenced by a representative plaintiff other than the complainant under this provision of the statute.

Section 106(1)(a) further limits the timing on when the cause of action may be brought until after the Commission has made a finding in an inquiry that the organization has contravened the CPPA. The finding must not have been appealed (and the time limit for an appeal must have expired) or the Tribunal has made a final decision on an appeal.

The second way an individual may commence a claim is set out in section 106(2) where an individual may claim against an organization that has been convicted of a listed offence under the CPPA (such as for failing to report a breach, failing to maintain records, or failing to retain personal information). As with the previous section, the individual commencing a claim must have been "affected by" the conduct giving rise to the conviction.

These statutory causes of action would arise only after there has been a finding by the Commission of a contravention or offence and the appeal period has expired. This allows companies to focus on responding to an inquiry by the Commission before turning to a defence of a civil claim if a breach of the CPPA is found

to have occurred. However, it means organizations should be very careful about the materials and information they provide to the OPC during the investigation, as plaintiff's counsel in a subsequent action may be able to obtain copies via an Access to Information Act request.

When may such an action be brought?

In addition to setting out the grounds for the private right of action, the CPPA also sets out when and where the action may be brought. The applicable limitation period is two years after the day on which the individual "becomes aware" of, under section 106(1), the Commissioner's finding, or the Tribunal's decision under section 106(2) of the conviction. This language could be interpreted to mean the actual knowledge of the individual asserting the claim rather than when the individual "knew or ought to have known" of the claim as set out in Canadian common law limitation statutes.

The plaintiff may decide which court to commence the CPPA claim, whether that is Federal Court or a provincial superior court. This does not, however, prohibit an organization from asserting a lack of jurisdiction argument that may be raised based on the parties involved and the nature of the underlying conduct.

There is no guidance provided on the type or quantum of damages that an individual may seek from an organization for a breach of the CPPA. The onus is on the plaintiff to prove that they have suffered some form of "loss or injury" as a result of the conduct of the organization. As under PIPEDA, what constitutes a compensable "loss or injury" in the context of a privacy breach is a topic of much debate.

How is this different from common law breach of privacy torts?

The CPPA private right of action would join a nascent body of jurisprudence in privacy litigation. Privacy torts, including intrusion upon seclusion and publicly placing a person in a false light, have been recognized by the Ontario Court of Appeal within the last decade. Consideration and application of these torts within Ontario and across common law provinces has gradually developed mainly in the area of privacy class actions.

There are some key differences between the statutory cause of action and the common law invasion of privacy torts. The first is that an individual asserting a private right of action may rely on the fact that the organization's conduct has already been found to be a breach of the CPPA through an investigation and inquiry by the OPC.

In contrast, a plaintiff asserting a common law breach of privacy tort does not have regulatory findings of fact to rely on but instead must prove the alleged acts or omissions occurred. For the tort of intrusion upon seclusion, the plaintiff must demonstrate that there was an unauthorized intrusion and that the intrusion was "highly offensive" to the reasonable person. Whether or not the intrusion was highly offensive will depend in part on the ability of the plaintiff to establish the defendant's motivations and objectives for engaging in the alleged conduct. Similarly, for the tort of placing a person in a false light, the plaintiff must establish the defendant had knowledge of, or acted in reckless disregard as to, the false light in which the plaintiff was placed. Proving these elements of the privacy tort will likely be more difficult than simply relying on a breach of the CPPA.

Another difference between the CPPA cause of action and privacy torts is the timing of when the claim may be commenced. The CPPA under section 106(1) would require an individual to wait to bring a claim until the OPC has made a finding of a contravention following an inquiry, or the Tribunal has made a finding of a contravention following an appeal. Similarly, under section 106(2), the organization must have been convicted of an offence under the CPPA before an individual can assert a cause of action arising from an organization's underlying conduct. Regulators are not known for the speed in which they operate and there is no reason to expect the OPC will be any different under the CPPA. This means an individual may wait years before an inquiry is complete and the appeals processes have run their course before they can commence a claim under the CPPA.

An individual asserting a claim for a common law privacy tort is not circumscribed by the same timing constraints. Oftentimes a privacy class action is commenced after a putative class member receives notice of a breach from an organization. At that stage, the organization has often not completed any internal investigations into the scope of the breach and the

OPC, if it has been notified, has often not completed an investigation or made any findings regarding contraventions. Class counsel may be motivated to file a claim first to assist with a potential carriage motion or other jurisdiction challenges.

Plaintiffs can be expected to bring claims both in privacy torts and private rights of action under the CPPA arising from an underlying breach. The findings by the OPC following an inquiry will likely form the basis for the facts asserted in such claims. However, it is likely that plaintiff's counsel, and class counsel in particular, will commence an action based on the information contained in a breach notification and amend the claim at a later date once the regulatory process is complete and a contravention or conviction has been found. On the other hand, if no such finding is made it may be difficult for the action to continue without findings of fact by a regulator made against the organization.

How is this different than statutory torts in provincial Privacy Acts?

Private rights of action have existed in Canadian law long before the proposed CPPA. Statutory torts for breach of privacy are set out in Privacy Acts in British Columbia, Manitoba, Saskatchewan and Newfoundland and Labrador. The Privacy Acts of these provinces contain a significant amount of parallel language. In general, it is a tort to violate a person's privacy "wilfully and without claim of right"; "proof of damages" is not a required element of the tort; and defences include consent, authorization by law, conduct in defence of person or property, and acts by journalists that are otherwise lawful.

The main point of departure between the CPPA private right of action and the Privacy Act torts is that the provincial Privacy Acts do not require the plaintiff to prove harm. In contrast section 106(1) of the CPPA requires an individual to have suffered damages for loss or injury "as a result of" the contravention or the conviction. This provision may lend itself to certification as a common issue of a class action as each class member may not have to prove individual harm arising from the privacy breach. Whereas the requirement to prove harm may be a hurdle for potential class actions seeking to demonstrate common issues at the certification stage.

Another difference is that under the Privacy Acts, the defendants may rely on the defence of consent, either express or implied, to the alleged breach. In a CPPA private right of action claim, the issue of consent will have been canvassed (and proven unsuccessful) at the inquiry or appeal stage leading to a finding of a breach. Instead an organization will likely defend the claim by asserting that the individual was too far removed from the underlying acts or omissions and that even if the individual proves they were affected by the contravention, they have failed to demonstrate resulting damage or loss.

In a typical data breach situation, it may also be difficult for plaintiff's counsel to meet the "wilfulness" requirement in the Privacy Acts. Where a bad actor deliberately directly breaches the privacy of an individual, the application of the Privacy Acts is clear. However, in most data breach matters, the organization itself is a victim of the bad actor, and it may be challenging to demonstrate that the organization and not the bad actor "wilfully" invaded the privacy of an individual.

Finally, a recent development in British Columbia may impact how privacy actions are commenced in the province. The Courts in British Columbia had consistently interpreted the Privacy Act to mean that because a statutory tort exists (and creates an exhaustive code relating to breaches of privacy) there is no common law tort for invasion of privacy recognized in the province. However, in the recent *Tucci v. Peoples Trust Company* decision, the BC Court of Appeal noted that there have been significant changes in the world, including the critical role that data has come to assume in people's lives. The Court concluded that it may be time to reconsider the issue of whether a common law tort of breach of privacy exists in conjunction with the statutory tort. However, no definitive ruling was made as the issue was not brought directly before the Court.

The CPPA private right of action is a statutory right of action, not a tort, and would likely not be seen to be in conflict with the common law or statutory torts for breach of privacy in the province. The impact however is that in certain provinces that have Privacy Acts, including British Columbia, an individual may choose to bring three claims arising from the same incident, including a common law tort, statutory tort, and assuming a finding by the Commission, a private right

of action under the CPPA. An organization will need to be prepared to address this litigation risk from an early stage following any privacy related incident.

Conclusion

The new rights in section 106 of the CPPA would give plaintiffs more options to sue when they think their privacy rights have been infringed. In addition to the existing common law and provincial Privacy Act claims, individuals "affected" by a breach of the CPPA or an offence under the CPPA would be able to sue.

The likely outcome is that more companies will find themselves the targets of more complex lawsuits. For instance, instead of a lawsuit that only claims under the common law torts, plaintiffs are more likely to sue for the common law torts as well as under the CPPA and, if applicable, the provincial Privacy Acts. Because each of these claims has slightly different elements, this gives plaintiffs more options – and makes it more complicated for companies to defend the lawsuits.

In addition, under the CPPA, the risk of a lawsuit is heightened as the CPPA would impose new and/or more stringent privacy requirements on organizations, meaning an increased likelihood of non-compliance that could trigger an investigation and potential claim under the CPPA.

Companies that are under investigation by the Commission will also need to be prepared for an even longer timeline to the end of lawsuits than is currently the case. Currently, plaintiffs (or class counsel) often start a lawsuit as soon as there is notification of a breach, and in many provinces they must start them within two years of notification. Investigations may happen in parallel to the litigation.

Under section 106 of the CPPA, lawsuits can be started up to two years after the investigation ends. Investigations themselves can take a number of years and so companies may find themselves waiting many years to know if any lawsuits will be brought.

CPPA: An in-depth look at the privacy policy provisions in Canada's proposed new privacy law

Bill C-11, the *Digital Charter Implementation Act*, was introduced on November 17, 2020. It proposes the new *Consumer Privacy Protection Act* (**CPPA**) as a replacement for the existing *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the federal legislation regulating privacy in the private sector.

This article addresses the CPPA's proposed changes to the accountability, openness and transparency obligations, with an overview of the requirements for privacy policies and what organizations must do to prepare in anticipation of the CPPA. An organization's privacy policy plays a vital role in its privacy compliance program, being the instrument by which the organization meets its openness and transparency obligations under the act.

Move away from permissive language to mandatory language

One of the key changes under Bill C-11 is the move away from principles-based PIPEDA (based on the OECD Principles, which found their way into a schedule to PIPEDA) to enacting actual language and obligations within the statute itself. While substantively very similar to the principles under Schedule 1 of PIPEDA, the provisions proposed in Bill C-11 will bring additional clarity about requirements for compliance, in part because much of the language of the Schedule in PIPEDA (should) would be replaced by clear requirements under the CPPA (must). For example, PIPEDA's Principles on accountability and openness hold organizations accountable and require them to make public and readily available detailed information on their policies and practices for the management of personal information. Under the CPPA, these principles are more clearly articulated, with concrete obligations for compliance.

New emphasis on privacy management programs under the CPPA

While not spelled out under PIPEDA, the concept of a privacy management program as demonstration of accountability through appropriate policies and procedures that promote good practices has appeared in previous guidance from the Office of the Privacy Commissioner of Canada (**OPC**). OPC guidance reflects the OPC's interpretation of PIPEDA, but is non-binding.

Whereas PIPEDA requires various standalone elements to address privacy concerns, the CPPA would speak (in section 9) in terms of a comprehensive "privacy management program." This program would have to include "policies, practices and procedures put in place to fulfil [the organization's] obligations" under the CPPA. The CPPA would also set out what types of policies, practices and procedures would be required to demonstrate accountability for the protection of personal information. These policies, practices and procedures must address the protection of personal information, as well as requests for information and complaints are received and dealt with. In addition, the CPPA would require that training and information be provided to the organization's staff respecting its policies, practices and procedures, along with the development of materials to explain the organization's policies and procedures put in place to fulfil its obligations under the CPPA.

The CPPA would also require that an organization's privacy management program must be proportionate to the volume and sensitivity of the personal information that the organizations control. A similar obligation exists in PIPEDA, but is more narrowly framed in terms of the form of consent and the safeguards protecting personal information needing to be appropriate to the sensitivity of the information.

In a new provision under the CPPA (section 109(e)), the OPC would also, on request by an organization, have to "provide guidance on the organization's privacy management program."

Readily available information presented in plain language

PIPEDA's Openness Principle requires organizations to make information about privacy policies and practices "readily available" to individuals. This requirement would be transposed into the CPPA, but would also create new standards for the type of information to be presented and the manner in which organizations must present such information to individuals.

While PIPEDA Principle 4.8.1 requires the information to be in a form that is "generally understandable," the new law would raise the bar and create a higher standard to make the information be available in "plain language." PIPEDA's "generally understandable" requirement begs the question of "understandable to who?" The CPPA requirement of "plain language" is less subjective, but will likely still create a challenge for organizations, considering the complexity of privacy management programs, as well as the various new rights and obligations to be introduced. However, it is not a new concept and this requirement to present information using "clear and plain language" is also present in the European General Data Protection Regulation (**GDPR**). A privacy policy that uses complex language, long documents resembling contracts and complicated legal concepts to explain the organization's privacy management program defeats the purpose of creating an instrument of transparency, openness and accountability. An incomprehensible privacy policy may also invalidate consent, if it is sufficiently comprehensible that the individual cannot be said to have understood what they were consenting to.

Additional information required

The Openness and Transparency provisions in the CPPA would also include a restructuring and restatement of the obligations under Principle 4.8.2 of PIPEDA, mandating the type of additional information that an organization must make available in fulfilling its obligations of openness and transparency under the CPPA. In privacy policies under the CPPA, organizations would need to:

a. Describe the type of personal information being handled.

   An obligation similar to current obligations under Principle 4.8.2(c), is to describe in the privacy policy the types of personal information that the organization collects, uses and discloses as part of its commercial activities. This obligation also extends to a description of information collected by the organization and then transferred to a service provider for processing, as the organization remains accountable for this personal information even after such a transfer.

b. Provide a general account of how the organization uses personal information, and application of any consent exceptions.

   This is another nod to the current obligation under PIPEDA's Principle 4.8.2(c). However, the CPPA would unpack the current obligation and introduce a further requirement to provide a general account of how the organization will apply exceptions to consent, should it choose to process personal information without the consent of the individual. The exceptions to the requirement for consent under the CPPA mirror current exceptions under PIPEDA, but the CPPA also introduces new broader ones, such as exceptions for certain enumerated business activities, for de-identifying personal information, for research and development within the organization (provided the information is first de-identified) and for socially beneficial purposes (if the information is first de-identified and the if the disclosure is to a government or health-care institution).

c. Provide a general account of the use of any automated decision system to make certain predictions, recommendations or decisions.

   This presents a new requirement for organizations that use such systems to make "predictions, recommendations or decisions" about individuals based on their personal information. In an effort to promote algorithmic transparency, organizations would be required to provide a general account of their uses of any automated decision system

used for the purpose of making predictions, recommendations or decisions that could have "significant impacts" on individuals. This disclosure would likely find a home in an organization's privacy policy.

The definition of "significant impacts" is not provided under the CPPA, which creates some ambiguity for organizations seeking to comply. It remains to be seen how any such impact will be measured and what level of impact will trigger the obligation to account for the use of such algorithmic systems in the privacy policy.

The CPPA falls short of the GDPR's prohibition on fully automated decision-making systems that result in a legal or similarly significant effect without consent of the individual or a prescribed legal authorization (the CPPA sidesteps the issue by using a definition that would capture any such system that "assists or replaces" human judgement). It is likely that under the CPPA, an automated decision-making system that resulted in legal consequences for an individual (e.g., predictive policing models) would be considered "significant." Less clear is whether a decision made by such automated systems to increase the price of certain goods or services in a particular area would qualify as "significant" and require disclosure in a privacy policy.

d. Provide information about international or interprovincial transfers or disclosure of personal information that may have reasonably foreseeable privacy implications.

   Personal information transferred to a different country becomes subject to that country's laws. Considering the purpose of the CPPA, which recognizes the importance for the flow of personal information across borders and geographical boundaries in economic activity, it is no surprise that a transparency requirement about international transfers is included. Nevertheless, not every international transfer must be flagged in the policy. Information about international and interprovincial transfers must be provided only if there are "reasonably foreseeable privacy implications," such as when the privacy and data protection legal framework in that foreign jurisdiction may impact the individual's rights to privacy. This is in line with current guidance from the OPC to include in the policy information about storage or transfers to a foreign jurisdiction.

e. Provide information about an individual's right to disposal of, or access to, their personal information.

   The CPPA would introduce new privacy rights for individuals, and as a result, the transparency obligations include the requirement for organizations to provide enough information for individuals to know how to exercise their new rights under the CPPA. Among these new rights is the right to request the disposal of personal information. For a further discussion of disposal rights and obligations, see our article here.

f. Provide contact information.

   The organization must make public the business contact information of a designated individual within the organization to whom complaints or requests may be directed. This is the same requirement as found in PIPEDA.

The current regime makes the organization accountable to the individuals whose information the organization collects, uses or discloses. Under the CPPA, the OPC would have the power to request access an organization's "policies, practices and procedures that are included in its privacy management program" (section 10). For this reason, organizations should consider establishing a clear understanding of what is, and what is not, within the privacy management program, to avoid having to disclose peripheral information or materials if asked.

Are there penalties for a non-compliant privacy policy?

Similar to the current regime, individuals will still be able to make complaints regarding non-compliance by organizations with the requirements under the CPPA, which could include a failure of an organization's privacy policy to meet Openness and Transparency standards. Such complaints will then be investigated by the OPC. The OPC can also initiate its own investigations into the organization's compliance.

Under the CPPA, the OPC's enforcement powers would be expanded, allowing the OPC to issue findings of contraventions of the CPPA and issue compliance orders. A compliance order may be issued to make an organization take certain measures to comply with the CPPA or stop doing something that is in contravention of the CPPA. With the new privacy regime, the OPC would be able to make recommendations that monetary penalties be imposed by the newly formed Tribunal.

Key contacts

Kirsten Thompson
Toronto
D +1 416 863 4362
kirsten.thompson@dentons.com

Kirsten Thompson is a partner in the Toronto office and is the national lead of the Transformative Technologies and Data Strategy group. She has both an advisory and advocacy practice, and provides privacy, data security and data management advice to clients in a wide variety of industries, and has been lead counsel on some of North America's largest data breaches and investigations. Read more here.

Contributing Authors

Anca Sattler

Anca Sattler is a senior associate at Dentons, working in the Firm's, Privacy and Cybersecurity group. Her privacy practice is broad and spans over transactional and investigation aspects of privacy, while helping her clients implement privacy compliance in their organization's day-to-day operation. Read more here.

Karl Schober

Karl Schober is a Senior Associate in Dentons' Privacy and Cybersecurity group, and Transformative Technologies and Data Strategy. Karl is a highly respected lawyer on all matters related to privacy law and data governance in the emerging technology sphere, including wearable devices, smart homes, connected and autonomous vehicles, smart cities and the Internet of Things. Read more here.

Luca Lucarini

Luca Lucarini is an associate in Dentons' Litigation and Dispute Resolution and Transformative Technologies groups. His practice focuses on privacy (in particular, health privacy) and cybersecurity, marketing and advertising, and general consumer protection laws and regulations. Read more here.

Chloe Snider

Chloe Snider is a partner in Dentons' Litigation and Dispute Resolution and Transformative Technologies groups. Chloe has a commercial litigation practice with an emphasis on privacy and technology disputes. Read more here.

Tracy Molino

Tracy Molino is counsel in Dentons' Banking and Finance group. She has particular interest in FinTech, PayTech and other innovative data-driven technologies in the financial services and payments sector. Read more here.

Kelly Osaka

Kelly Osaka is a partner in Dentons' Calgary office, and is a member of the Litigation and Dispute Resolution group and the Privacy and Cybersecurity. Kelly's is an experienced litigator, with a particular expertise in class actions, privacy law claims and regulatory investigations. Read more here.

Julie Facchin

Julie Facchin is counsel in the Litigation and Dispute Resolution group. Based in Vancouver, she maintains a commercial litigation practice with particular emphasis on class action defence and privacy law. Julie helps clients navigate privacy breaches and address other privacy or access to information issues. Read more here.

Sasha Coutu

Sasha Coutu is an articling student in Dentons' Ottawa office. She has a Master's degree in health informatics and previously worked as an investigator in the Office of the Privacy Commissioner of Canada.

Noah Walters

Noah Walters is an articling student in Dentons' Toronto office. He has a special interest in emerging technologies and blockchain-based businesses.

Related Practice Leads:

Chantal Bernier

National Lead Dentons' Canada Region Privacy and Cybersecurity practice group

Gord Tarnowsky

National Lead Dentons' Canada Region Litigation and Dispute Resolution group

ABOUT DENTONS

Dentons is the world's largest law firm, connecting talent to the world's challenges and opportunities in more than 75 countries. Dentons' legal and business solutions benefit from deep roots in our communities and award-winning advancements in client service, including Nextlaw, Dentons' innovation and strategic advisory services. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and world-class talent challenge the status quo to advance client and community interests in the New Dynamic.

dentons.com

CSBrand-47557-Guide-to-C-11_05 — 27/01/2021