THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Digital Charter Implementation Act

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW SECTION

November 2021

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Privacy and Access Law Section, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Privacy and Access Law Section.

TABLE OF CONTENTS

Digital Charter Implementation Act

Digital Charter Implementation Act

I. INTRODUCTION

Bill C-11, the *Digital Charter Implementation Act, 2020,* was introduced in November 2020 and died on the Order Paper with the call of the 2021 election. The Canadian Bar Association's Privacy and Access Law Section (CBA Section) offers its comments on Bill C-11 now, in anticipation that another bill will be introduced in the current Parliament. The CBA Section represents specialists in privacy law and access to information issues from across Canada. In December 2019, the CBA Section responded to Innovation, Science and Economic Development Canada's (ISED) consultation document, *Strengthening Privacy for the Digital Age*[1] (December 2019 submission).

The CBA Section is generally supportive of Bill C-11. We address matters that could result in unintended consequences if the bill were reintroduced as proposed. We comment on the following issues:

- De-identification
- Business Transaction Exemption
- Interprovincial Data Flows
- Interim Orders
- Final Orders
- Penalty Recommendations
- Procedural Fairness at the Inquiry Stage
- Procedural and Substantive Fairness at the Tribunal
- Automated Decision-Making Systems
- Sensitive Information
- Private Right of Action

---

1 Strengthening Privacy for the Digital Age: Response to Proposals to Modernize PIPEDA, online.

The definitions in Bill C-11 that are relied upon in those comments follow below.

II. DEFINITIONS

Application

6 (1) This Act applies to every organization in respect of personal information that

(a) the organization collects, uses or discloses in the course of commercial activities; or

(b) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business;

(4) This Act does not apply to

(a) any government institution to which the Privacy Act applies;

(b) any individual in respect of personal information that the individual collects, uses or discloses solely for personal or domestic purposes;

(c) any organization in respect of personal information that the organization collects, uses or discloses solely for journalistic, artistic or literary purposes;

(d) any organization in respect of an individual's 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; or

(e) any organization that is, under an order made under paragraph 119(2)(b), exempt from the application of this Act in respect of the collection, use or disclosure of personal information that occurs within a province in respect of which the order was made.

De-identification of personal information

20 An organization may use an individual's personal information without their knowledge or consent to de-identify the information.

Research and development

21 An organization may use an individual's personal information without their knowledge or consent for the organization's internal research and development purposes, if the information is de-identified before it is used.

Socially beneficial purposes

39 (1) An organization may disclose an individual's personal information without their knowledge or consent if

(a) the personal information is de-identified before the disclosure is made;

(b) the disclosure is made to

(i) a government institution or part of a government institution in Canada,

(ii) a health care institution, post-secondary educational institution or public library in Canada,

(iii) any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or

(iv) any other prescribed entity; and

(c) the disclosure is made for a socially beneficial purpose.

Policies and practices

62 (1) An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfil its obligations under this Act.

Additional information

(2) In fulfilling its obligation under subsection (1), an organization must make the following information available:

(c) a general account of the organization's use of any automated decision system to make predictions, recommendations or decisions about individuals that could have significant impacts on them;

(d) whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications;

Information and access

63 (1) On request by an individual, an organization must inform them of whether it has any personal information about them, how it uses the information and whether it has disclosed the information. It must also give the individual access to the information.

Automated decision system

(3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained.

Contravention

82 (1) An individual may file with the Commissioner a written complaint against an organization for contravening Part 1.

Commissioner may initiate complaint

(2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act, the Commissioner may initiate a complaint in respect of the matter.

Time limit

(3) A complaint that results from the refusal to grant a request made under section 63 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.

Notice

(4) The Commissioner must give notice of a complaint to the organization against which the complaint was made, unless the Commissioner decides under subsection 83(2) not to carry out an investigation.

Investigation of complaint by Commissioner

83 (1) The Commissioner must carry out an investigation in respect of a complaint, unless the Commissioner is of the opinion that

(a) the complainant should first exhaust grievance or review procedures otherwise reasonably available;

(b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under any federal law, other than this Act, or provincial law;

(c) the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose; or

(d) the complaint raises an issue in respect of which a certification program that was approved by the Commissioner under subsection 77(2) applies and the organization is certified under that program.

Nature of inquiries

90 (1) Subject to subsection (2), the Commissioner is not bound by any legal or technical rules of evidence in conducting an inquiry and must deal with the matter as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit.

Restriction

(2) The Commissioner must not receive or accept as evidence anything that would be inadmissible in a court by reason of any privilege under the law of evidence.

Opportunity to be heard

(3) In conducting the inquiry, the Commissioner must give the organization and the complainant an opportunity to be heard and to be assisted or represented by counsel or by any person.

Decision

92 (1) The Commissioner must complete an inquiry by rendering a decision that sets out

(a) the Commissioner's findings on whether the organization has contravened this Act or has not complied with the terms of a compliance agreement;

(b) any order made under subsection (2);

(c) any decision made under subsection 93(1); and

(d) the Commissioner's reasons for the findings, order or decision.

Compliance order

(2) The Commissioner may, to the extent that is reasonably necessary to ensure compliance with this Act, order the organization to

(a) take measures to comply with this Act;

(b) stop doing something that is in contravention of this Act;

(c) comply with the terms of a compliance agreement that has been entered into by the organization; or

(d) make public any measures taken or proposed to be taken to correct the policies, practices or procedures that the organization has put in place to fulfil its obligations under this Act.

Powers of Commissioner

98 (1) In carrying out an investigation of a complaint, conducting an inquiry or carrying out an audit, the Commissioner may

(d) make any interim order that the Commissioner considers appropriate;

Disposition of appeals

102 (1) The Tribunal may dispose of an appeal by dismissing it or by allowing it and, in allowing the appeal, the Tribunal may substitute its own finding, order or decision for the one under appeal.

Standard of review

(2) The standard of review for an appeal is correctness for questions of law and palpable and overriding error for questions of fact or questions of mixed law and fact.

Promoting purposes of Act

109 The Commissioner must

(c) undertake and publish research that is related to the protection of personal information, including any research that is requested by the Minister;

III. DE-IDENTIFICATION

The sections on de-identifying personal information can have significant operational consequences for organizations and for the innovation economy.

The CBA Section supports the clarification in the proposed *Consumer Privacy Protection Act* (CPPA) that organizations may de-identify personal information without the consent of the individual (s. 20) and use that information for internal research and development (s. 21).

The CBA Section has concerns about the inability to share de-identified personal information with other organizations without the knowledge or consent of the individual except when shared to a certain limited class of organizations for socially beneficial purposes (s. 39(1)).

We recognize that the government may be motivated to restrict sharing because of its concern that the recipient organization may attempt to re-identify personal information. The CBA Section shares this concern. However, this "evil" has been addressed by the CPPA in two ways. First, the CPPA makes re-identification an offence (s. 75) punishable by a fine of up to the greater of $25,000,000 and 5% of gross global revenue. Second, any re-identification constitutes a collection and is subject to the requirements of obtaining the knowledge and consent of the individual as well as to other sections of the CPPA applicable to personal information.

The CBA Section is troubled by the proposed wording of the definition to de-identify because it sets too high a threshold for what constitutes de-identified personal information. The result is that many ordinary business activities involve disclosures that will be prohibited without consent. If that definition is replaced with a threshold for de-personalizing information that is similar to "pseudonymisation" under the General Data Protection Regulation[2] (GDPR), the proposed scheme would be more coherent, and we would support it.

The root problem, in the CBA Section's view, is that the definition of de-identify results in de-identified personal information not being personal information at all:

> 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.

Personal information that is modified to ensure that it does not identify an individual is no longer personal information. It is anonymized information that is not currently subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and should not be subject to CPPA or any law governing personal information. It is inappropriate to include this concept in the definition of de-identify as it expands the scope of the law to include anonymized information. Further, comingling the concepts of anonymized information and de-identified information will create interpretative difficulty and international legal compliance challenges.

---

2 (EU) 2016/679

Read literally in its ordinary, grammatical sense, an algorithm processing data to develop a statistic is a process of de-identification. If that algorithm produces a statistic that 40% of shoppers buy ten or more items a year in at least two visits to a website, that is de-identified personal information. The disclosure of that statistic would be contrary to the CPPA. This would be a troubling result.

The second aspect of the definition is also problematic. The threshold requires no reasonably foreseeable circumstance in which the information can be re-identified. Again, the result is that the CPPA attempts to regulate what will in many cases not be personal information because while re-identification may be foreseeable, there may be no serious possibility of re-identification. For example, one can reasonably foresee that computing power will continue to multiply exponentially so that new forms of re-identification will be possible in the future, while there is no serious possibility of re-identification now.

By contrast, the concept of "pseudonymisation" in the GDPR contemplates a threshold of data that can, in fact, be re-identified with other information. Accordingly, there are strong policy reasons for limiting the disclosure of this information without consent except for socially beneficial purposes to a limited class of organizations. Article 4(5) of the GDPR defines pseudonymisation:

> 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

To the extent that the CPPA proposes to regulate a category of personal information that is not directly identifiable but can be re-identified when combined with other data, the CBA Section believes that the pseudonymisation standard of the GDPR is more consistent with the intent of the CPPA and the risks it attempts to address.

RECOMMENDATIONS:

1. **Revise the definition of de-identify to (1) avoid incorporating anonymized information and (2) align with the concept of pseudonymisation in the GDPR.**

IV. BUSINESS TRANSACTION EXEMPTION

The requirement that information be de-identified to be shared during a business transaction (CPPA, s. 21(1)(a)) is unworkable in practice. As noted above, the threshold for de-identification sets too high a bar for this to be practicable.

In any event, during mergers and acquisitions, investment and other commercial transactions, it is frequently necessary to disclose some personal information to a potential buyer to perform due diligence and determine whether to proceed with the transaction. For example, the personal information of senior or key employees of the organization being sold (such as contractual terms of compensation or consequences of early termination) are typically given to prospective buyers for this purpose. These individuals may not be privy to the contemplated transaction.

Similarly, once the parties enter into a purchase agreement, it is often necessary to give the buyer additional personal information to prepare for closing and ensure a seamless transition to the new owner. For example, in an asset transaction, the buyer would require employee personal information to make employment offers to those employees. There may also be similar instances when certain customer information is shared (e.g., to assess overlap of customer lists, value of list).

Section 7.2 of PIPEDA introduced in 2015 has worked well. The CBA Section is not aware of any Office of the Privacy Commissioner (OPC) investigations or decisions where abuse of personal information disclosed under these provisions is mentioned. Section 7.2 of PIPEDA already limits personal information that can be shared and limits its use. PIPEDA requires safeguards and an obligation to return or destroy the information if a transaction does not proceed or, if it does, to advise the affected individual of the transfer.

Consent is not a realistic basis on which to disclose personal information for a potential transaction. A contemplated transaction can be confidential for appropriate business reasons (and securities law requirements). Seeking consent in those cases undermines the necessary confidentiality of the transactions. Furthermore, obtaining consent may be impracticable in the circumstances of most business transactions and a refusal of consent may thwart a potential business transaction.

RECOMMENDATION:

2. Remove the requirement in s. 21(1)(a) of the CPPA that information must be de-identified to be shared in the course of a business transaction.

V. INTERPROVINCIAL DATA FLOWS

The CBA Section questions the reference to interprovincial data flows in s. 62(2)(d) of the CPPA. It is unclear what harm that section addresses by requiring disclosure of certain interprovincial data flows. The CPPA will apply to interprovincial transfers. The OPC will retain jurisdiction. Orders of the OPC and the tribunal are registrable in Federal Court and are enforceable in every province and territory in Canada. The CBA Section suggests that this requirement for interprovincial transfers be removed from the CPPA. There should be no barriers to interprovincial trade and commerce.

RECOMMENDATION:

3. Remove references to interprovincial transfers in s. 62(2)(d) of the CPPA.

VI. INTERIM ORDERS

The CBA Section is concerned about the breadth of the OPC's interim order power in section 98(1)(d) of the CPPA. Since OPC inquiries are complaint-driven, they can investigate an industry common practice. If the OPC enjoins the action at an early stage and takes several months, or even years, to render a decision, there can be significant implications for an organization's competitiveness.

As described below, the CBA Section questions the ability of a multi-mandated OPC to implement appropriate procedural fairness. Extraordinary powers like cessation orders require exacting procedural fairness standards, including narrow applicable time periods and the opportunity for the respondent organization to promptly challenge the action. Courts and moving parties must meet high standards – such as under the *RJR MacDonald Inc. v. Canada (Attorney General)*[3] test for injunctions – to exercise these powers. The CPPA does not structure the OPC to meet such strict standards of fairness.

[3] 1994, 1 SCR 311.

In our December 2019 submission, the CBA Section stated that:

> As extreme powers, cessation and records preservation orders are usually not appropriate for an ombudsman model. However, those powers might be extended to the OPC and reserved for egregious cases including imminent material harm to individuals. They should not be available to challenge normal business practices or differences of opinion or interpretation. Careful consideration should be given to the timing to exercise these new powers and any right to appeal.

We continue to be of this view. Interim orders should be issued by the Tribunal.

To the extent that the OPC is concerned about evidence spoliation pending an investigation, existing obstruction offences can be pursued. The OPC can also seek a preservation order from the courts in egregious cases where an imminent risk of spoliation exists.

RECOMMENDATION:

4. Remove the OPC's interim order-making powers.

VII. FINAL ORDERS

Various CPPA provisions deem the OPC to be an advisor to organizations (s. 109(e)), a complainant (s. 82(2)), an investigator (ss. 82-83) and an adjudicator (s. 92). Even if it were possible to achieve procedural and substantive fairness for organizations and individuals with these multiple roles, it requires a strict segregation of duties. The Commissioner would only have the role of an administrator since he or she should not at the same time be advisor, complainant, investigator and adjudicator.

These fairness concerns are far from academic. The Canadian Judicial Council's experience with its disciplinary process under the *Judges Act* shows that these multiple roles are incompatible within the same organization, and can hinder fairness, efficiency and cost-effectiveness as challenges to these structures will repeatedly be an issue for the courts on judicial review.

Ultimately, the CBA Section believes that the OPC's role should not include adjudicative functions. Like its role with respect to penalties proposed in Bill C-11, the OPC should be empowered to make recommendations for orders to the Tribunal. The Tribunal should then adjudicate those recommendations on the merits or, if the organization consents to the recommendations, issue a consent order.

RECOMMENDATION:

5. **Remove the order-making powers of the OPC and include a power to recommend orders to the Tribunal and obtain a consent order if the organization agrees to the recommendation.**

VIII. PENALTY RECOMMENDATIONS

The CBA Section believes that the CPPA's penalty provisions can be clarified in two respects. First, it is not clear whether the OPC is empowered to make a (non-binding) recommendation on the quantum of a penalty. We believe the OPC should make those recommendations. Second, the OPC and the organization should be able to agree to a penalty, which can become part of the Tribunal's consent order.

RECOMMENDATIONS:

6. **State that the OPC may recommend a quantum of the penalty to the Tribunal.**
7. **Provide that (1) the organization and OPC may jointly recommend a penalty to the Tribunal; (2) the Tribunal may hear from interested parties before accepting a joint recommendation; and (3) the Tribunal ought to accept a joint recommendation unless it finds it is contrary to the public interest.**

IX. PROCEDURAL FAIRNESS AT THE INQUIRY STAGE

Although the CBA Section finds that the OPC's adjudicative role is inconsistent with its other roles, we wish to comment on procedural fairness in the event Bill C-11 is reintroduced as drafted.

The CPPA does not adequately offer robust protection for procedural fairness during the inquiry phase. Section 90(3) gives organizations "an opportunity to be heard," but more detail about those participation rights is required. At a minimum, the CPPA should establish seven basic core principles of procedural fairness:

1. The right of the complainant to participate and give evidence;
2. The circumstances in which an oral hearing may be requested by the organization or the individual;
3. The right to disclosure of evidence against the organization, including the submissions of investigation staff;
4. The right to produce witnesses and documentary evidence;

5. The right to give expert evidence;
6. The right to challenge evidence against the organization;
7. Parameters for addressing requests from third parties to intervene.

RECOMMENDATION:

8. Include minimum procedural fairness protections that the OPC must address in its procedural code for inquiries.

X. PROCEDURAL AND SUBSTANTIVE FAIRNESS AT THE TRIBUNAL

The CBA Section supports the creation of the Personal Information and Data Protection Tribunal (Tribunal). However, more attention should be paid in the *Personal Information and Data Protection Tribunal Act* (PIDPTA) to ensuring procedural and substantive fairness.

Regulatory models that include tribunals benefit significantly from members with subject matter expertise. This is particularly important in the complicated and quickly changing field of privacy law. At least half the Tribunal members should have experience in information and privacy law and understand the unique implications of the area (s. 6(4)).

As with the CBA Section's recommendations on procedural fairness at the inquiry stage, we believe that the minimum procedural protections addressed by the Tribunal's code of practice be enumerated in PIDPTA. At a minimum, it should establish seven basic core principles of procedural fairness:

1. The right of the complainant to participate and give evidence;
2. The presumption of an oral hearing, or at a minimum the circumstances in which an oral hearing may be requested by the organization or the individual;
3. The right to disclosure of evidence against the organization, including the submissions of investigation staff;
4. The right to produce witnesses and documentary evidence;
5. The right to give expert evidence
6. The right to challenge evidence against the organization;
7. Parameters for addressing requests from third parties to intervene.

These principles accord with procedural fairness protections established by other tribunals, such as the Competition Tribunal, in Part 2 of the *Competition Tribunal Rules.*[4]

4 SOR-2008-141

The CBA Section believes that the standard of review (SOR) identified in s. 102(2) of the CPPA for appeals from an OPC inquiry to the Tribunal is appropriate. Section 102(2) is consistent with the applicable SOR prescribed by the majority of the Supreme Court of Canada in *Canada (Minister of Citizenship and Immigration)* v. *Vavilov*[5] (i.e., appellate standards of review for an appeal from an administrative decision).

However, the applicable standard of judicial review of Tribunal decisions before the Federal Court should be set out in PIDPTA. Section 21 states that Tribunal decisions are final and binding except for judicial review under the *Federal Courts Act*. PIDPTA does not specify a SOR for that judicial review process.

RECOMMENDATIONS:

9. **The Tribunal should be composed of at least 50% of members with privacy expertise.**
10. **The Tribunal should be composed of at least 50% of members with judicial or comparable adjudicative expertise.**
11. **Make the introduction of rules for hearings, which are currently permissive in PIDPTA s. 19, mandatory, and require that those rules include minimum procedural fairness protections.**
12. **Provide for an applicable standard of review for judicial review of decisions of the Tribunal.**

XI. AUTOMATED DECISION-MAKING SYSTEMS

The CBA Section agrees with the creation of a regulatory framework for certain types of automated decision-making systems. However, intersecting issues of privacy, equity, anti-discrimination and competition related to automated decision-making require a careful, comprehensive and nuanced approach to regulation. Addressing the intersection of these issues goes beyond what can be accomplished in consumer privacy legislation.

The challenges of addressing automated decision-making systems in privacy legislation are illustrated by the inadequate individual rights under the CPPA. Individuals have a right to receive general disclosure of how automated decision systems are used (s. 62(2)(c)) and, as

5 2019 SCC 65

part of an access request, an explanation of the prediction, recommendation or decision and use of the personal information that was obtained (s. 63(3)). However, these rights do not assist an individual who believes they have been treated unfairly. There is no mechanism to challenge the result.

Further, the definition of "automated decision system" in the CPPA is so broad as to sweep in many digital practices that are commonplace and lack any inherent harm. Specifically, there are two issues with the definition:

- the inclusion of any technology that "assists" judgment of human decision-makers casts a large web to catch decisions that are, by their nature, not automated decisions; and
- "rules-based systems" are nearly ubiquitous in our increasingly digital world (e.g., a customer service system that automatically routes calls to the right department, forwarding IP addresses to geographically relevant web addresses)

As a result, the proposed definition operates to find an automated decision system nearly anywhere that a digital device is used to assist a person exercise their judgment.

The CBA Section is concerned that individual rights with respect to automated decision-making are chimerical and that organizations' obligations (given the breadth of the definition) are too onerous. We believe that individuals and organizations are better served by standalone legislation that addresses the multifaceted nature of harms associated with automated decision-making. However, recognizing that some regulation of this area is likely to proceed in the CPPA, the definition of automated decision systems should be narrowed and the scope of obligations on organizations should be focused on automated decision-making systems that have significant impacts on the individual.

RECOMMENDATIONS:

13. **Revise the definition of automated decision systems to focus on technology that makes assessments or decisions in lieu of human decision-making.**
14. **Clarify that the obligations on organizations in sections 62(2) and 63(3) apply to automated decision-making that has a material impact on, or poses a risk of significant harm to, the individual.**

XII. SENSITIVE PERSONAL INFORMATION

Personal information sensitivity is a key concept in the CPPA as illustrated by Bill C-11 explicitly referring to sensitivity in multiple sections:

- privacy management programs (s. 9)
- appropriateness of purposes (s. 12)
- forms of consent (s. 15)
- business transactions (s. 22)
- appropriate security safeguards (s. 57)
- breaches of security safeguards (s. 58)
- access rights to medical information (s. 66)
- safeguards for de-identification of personal information (s. 74)
- exercise of Commissioners powers and performance of Commissioner's duties and functions (s. 108)

The sensitivity of information is also indirectly implicated in the determination of penalties (s. 93). Although it is a key concept, there is no textual guidance to interpret sensitivity in the CPPA.

By contrast, PIPEDA explicitly requires a contextual assessment of the sensitivity of personal information. Sensitivity depends on the context in which information is collected, used, stored or communicated, although some categories of information are considered sensitive in almost every instance. For example, Principle 4.3 of PIPEDA states:

> Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

There is no similar directive in the CPPA.

Some jurisdictions, like the European Union, enumerate specific "special categories" of personal information for which processing is prohibited unless it falls into an exception. These categories include "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic

data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[6]

PIPEDA and legislation in some other jurisdictions have taken a principled approach to defining sensitive information. Quebec's Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, for example, deems information sensitive "if due to its nature or the context of its use or communication, it entails a high level of reasonable expectation of privacy."[7]

Overall, the CBA Section recommends continuing with a contextual, principle-based approach to determining the sensitivity of personal information.

RECOMMENDATIONS:

15. **Provide for a contextual assessment of the sensitivity of personal information which may consider the nature of the data, the purposes for which it is provided, the source from which it is obtained and whether the individual made it public themselves.**
16. **Include a non-exhaustive list of factors and examples to be considered in the contextual assessment, such as whether the personal information is about a person's biographical core, is impossible or extremely difficult to alter and whether the use or disclosure of the information would create a real risk of significant harm to the individual.**

XIII. PRIVATE RIGHT OF ACTION

It would be helpful to address the interaction between common law, civil law and provincial statutory causes of action and the private right of action under s. 106 of the CPPA.

There is an active privacy civil litigation practice across Canada, and courts have been asked to address potential conflicts between provincial statutory causes of action and common law claims.

---

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 9.

7 Bill 64, s. 102, amending Act respecting the protection of personal information in the private sector, CQLR c P-39.1, s. 12.

The CBA Section believes that it cannot be the government's intent to interfere with civil rights in a province based on the common law, civil law or provincial statutory causes of action even if the same conduct is a violation of the CPPA.

In many provinces, the limitation period for a claim is two years. However, the OPC cannot render a decision until that period is almost up (given the OPC's power to extend the time for inquiry to up to two years) and then the matter can go to the Tribunal.

As a result, it is likely that proceedings will be bifurcated so the same conduct that is both a CPPA violation and a violation of common law, civil law or provincial statutes results in multiple proceedings, with a risk of inconsistent results and placing organizations in double-jeopardy. This disconnect could also hinder the swift resolution of common law claims, as organizations will be reluctant to settle without certainty that a cause of action under the CPPA will not become actionable once the administrative procedure has been completed.

Importantly, the private right of action appears to create a cause of action for breach of statutory duty under the CPPA. This would significantly alter the existing common law on privacy torts and breach of statutory duty and warrants more serious consideration and consultation.

RECOMMENDATIONS:

17. **More study is required to consider whether the private right of action is appropriate.**

18. **If a private right of action is enacted, the procedural and substantive intersection between common law claims, administrative proceedings and statutory claims should be explicitly addressed.**

XIV. SUMMARY OF RECOMMENDATIONS

1. **Revise the definition of de-identify to (1) avoid incorporating anonymized information and (2) align with the concept of pseudonymisation in the GDPR**.

2. **Remove the requirement in s. 21(1)(a) of the CPPA that information must be de-identified to be shared in the course of a business transaction.**

3. **Remove references to interprovincial transfers in s. 62(2)(d) of the CPPA.**

4. **Remove the OPC's interim order-making powers.**

5. **Remove the order-making powers of the OPC and include a power to recommend orders to the Tribunal and obtain a consent order if the organization agrees to the recommendation.**

6. **State that the OPC may recommend a quantum in respect of the penalty to the Tribunal.**

7. **Provide that (1) the organization and OPC may jointly recommend a penalty to the Tribunal; (2) the Tribunal may hear from interested parties before accepting a joint recommendation; and (3) the Tribunal ought to accept a joint recommendation unless it finds it is contrary to the public interest.**

8. **Include minimum procedural fairness protections that the OPC must address in its procedural code for inquiries.**

9. **The Tribunal should be composed of at least 50% of members with privacy expertise.**

10. **The Tribunal should be composed of at least 50% of members with judicial or comparable adjudicative expertise.**

11. **Make the introduction of rules for hearings, which are currently permissive in PIDPTA s. 19, mandatory, and require that those rules include minimum procedural fairness protections.**

12. **Provide for an applicable standard of review for judicial review of decisions of the Tribunal.**

13. **Revise definition of automated decision systems to focus on technology that makes assessments or decisions in lieu of human decision-making.**

14. **Clarify that the obligations on organizations in sections 62(2) and 63(3) apply to automated decision-making that has a material impact on, or poses a risk of significant harm to, the individual.**

15. **Provide for a contextual assessment of the sensitivity of personal information which may consider the nature of the data, the purposes for which it is provided, the source from which it is obtained and whether the individual made it public themselves.**

16. **Include a non-exhaustive list of factors and examples to be considered in the contextual assessment, such as whether the personal information is about a person's biographical core, is impossible or extremely difficult to alter and whether the use or disclosure of the information would create a real risk of significant harm to the individual.**

17. **More study is required to consider whether the private right of action is appropriate.**

18. **If a private right of action is ultimately enacted, the procedural and substantive intersection between common law claims, administrative proceedings and statutory claims should be explicitly addressed.**