THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Bill C-27, Digital Charter Implementation Act, 2022

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW SECTION

October 2022

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 37,000 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

Bill C-27, Digital Charter Implementation Act, 2022

Bill C-27, Digital Charter Implementation Act, 2022

I. INTRODUCTION

The Canadian Bar Association's Privacy and Access Law Section (CBA Section) welcomes this opportunity to offer its views on Bill C-27, the *Digital Charter Implementation Act, 2022,* which would enact the *Consumer Privacy Protection Act* (CPPA), the *Personal Information and Data Protection Tribunal Act* and the *Artificial Intelligence and Data Act.* We comment more particularly on the CCPA and the *Personal Information and Data Protection Tribunal Act,* focusing on areas of significant concern. The CBA Section is generally supportive of the CPPA but believes that amendments are urgently required for the following issues:

- De-identification / Anonymization
- Disposal
- Procedural Fairness at the OPC and the Tribunal
- Automated Decision-Making Systems
- Transparency
- Sensitive Personal Information

II. DE-IDENTIFICATION AND ANONYMIZATION

The CPPA introduces for the first time, in federal private sector privacy legislation, specific definitions of "de-identified" personal information and "anonymized" information that for the past two decades have been interpreted by business, the Office of the Privacy Commissioner (OPC) and the courts in a commonly understood manner. The CBA Section supports introducing the concept of de-identification and clarifying that consent is not required for the act of de-identifying data. However, the proposed legal threshold for anonymization overturns Federal Court case law and will be practically impossible to meet. The federal government gives no rationale for this change to the law.

Subsection 2(1) of the *Personal Information Protection and Electronic Documents Act*, (PIPEDA)[1] defines "personal information" as "information about an identifiable individual" ("Tout renseignement concernant un individu identifiable").

---

1 SC 2000, c 5

In the Federal Court of Appeal decision in *Canada (Information Commissioner) v. Canada (Canadian Transportation Accident Investigation and Safety Board)*,[2] Justice Desjardins states about the definition of "personal information" in the *Privacy Act*,[3] which is equivalent to that in PIPEDA:

> These two words, "about" and "concernant", shed little light on the precise nature of the information which relates to the individual, except to say that information recorded in any form is relevant if it is "about" an individual and if it permits or leads to the possible identification of the individual. There is judicial authority holding that an "identifiable" individual is considered to be someone whom it is **reasonable to expect can be identified** from the information in issue when combined with information from sources otherwise available …

Information is thus not personal information if it is not reasonable to expect the individual could be identified from it or its combination with other information from sources otherwise available.

A year later, the Federal Court interpreted the definition of "personal information" in the *Privacy Act* and concluded that there must be a "serious possibility" of identifying an individual through the information alone or combined with "other available information."[4] This threshold was advocated by the OPC. Again, "impossibility" was not an appropriate threshold. More recently, the Federal Court found "serious possibility" and "reasonable to expect" are effectively the same thing: more than mere speculation or possibility.[5]

PIPEDA restricts the collection, use and disclosure of information if it is reasonable to expect or there is a serious possibility that an individual could be identified from that information or that information in combination with other information. If that threshold is not met, then the information is not personal information for the purposes of the legislation even if there is some residual risk of identification.

The proposed CPPA retains the existing definition of personal information, but adds two more concepts.

- De-identify "means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains."[6]

---

2 2006 FCA 157 at para 43, leave to appeal to SCC refused, 2007 CanLII 11607.

3 RSC 1985, c P-21.

4 *Gordon v Canada (Health)*, 2008 FC 258 at para. 34.

5 *Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness)*, 2019 FC 1279 at para. 53-54.

6 CPPA, s. 2(1).

- Anonymize "means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means."[7]

To "de-identify" information, the organization removes direct identifiers. However, the information would likely remain personal information under the existing interpretation of "personal information" because the information could be combined with other information to identify or re-identify the individual. Protection of an individual's privacy interests requires that this type of information remains subject to CPPA.

The CPPA also introduces the concept of "anonymized information" with an impossible test to meet. It is unclear why this definition is required. Its effect is to overturn the existing jurisprudence. Requiring an organization "to ensure that no individual can be identified from the information, whether directly or indirectly, by any means" is essentially a threshold of impossibility for most Canadian organizations. It may be possible for the largest organizations to hire data scientists to anonymize datasets but even those organizations will have trouble giving the assurance required by the CPPA.

The federal government has not advanced any argument for the necessity of this threshold to protect Canadians. If the risk of identification is speculative, so is any risk of harm to individuals. This issue is not merely academic. Organizations may wish to share information across industries to develop better insights or develop better toolsets. Obtaining consumer consent is impractical in these situations because the data may be historical. Also, organizations may wish to continue to avail themselves of possibly anonymizing information to meet their disposition obligations under CPPA, as they have done for over two decades under PIPEDA. There must be a threshold where the risk of harm to the individual is so speculative, that the organization's interest can be met in these circumstances.

RECOMMENDATION:

1. **The CBA Section recommends that the definition of "anonymize" be amended to be more consistent with existing case law and to balance risks of harm to individuals against achievable industry practices:**

   Anonymize means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to

[7] CPPA, s. 2(1).

ensure that <u>there</u> is no <u>reasonably foreseeable risk in the circumstances</u> that an individual can be identified from the information, whether directly or indirectly, by any means. (suggested amendments underlined)

III. DISPOSAL AT INDIVIDUAL'S REQUEST – SECTION 55

Under PIPEDA, an organization usually corrects or deletes personal information in its files or systems further to an individual's access request. Otherwise, personal information is deleted or anonymized because of normal information management processes and PIPEDA obligations that require organizations to dispose or anonymize personal information after it is no longer necessary for identified purposes.

Section 55(1) of CPPA proposes a new explicit right for individuals to request disposal of their personal information in specific circumstances and, in s. 55(2), a corresponding explicit obligation for organizations to dispose of the information with specific exceptions to that obligation.

The CBA Section has several concerns with the wording of some exceptions to the obligation to dispose in s. 55(2). For example, there is no exception to respond to a disposal request that reflects the need to retain personal information for clearly recognized reasonable business purposes, such as fraud prevention or detection, security and investigations.

Another exception to the disposal obligation that raises concern relates to "reasonable terms of a contract". While intended to assist organizations via a practical business exception, this exception is problematic as worded. What terms will be considered reasonable? Further uncertainty arises since not all impacted individuals will be party to a contract. Dealing with contracts with existing customers may also be problematic.

For access requests, there are other permitted exceptions for refusal to respond or for nondisclosure of reasons relating to those requests in s. 70, and several of them may be relevant in this context as well to avoid compromising investigations. There is no guarantee that individuals will, in all cases, make an access request before making a disposal request, and there is no option to not offer the reasons for refusal. Finally, there is no provision for the possibility of prescribing additional exceptions through regulation.

Many other CPPA provisions apply to safeguard personal information and impact retention and disposal obligations. For example:

- additional transparency obligations re: general account of use of exceptions, retention periods for sensitive data;

- section 18 requires an assessment and relevant measures/mitigations;
- retention periods already need to factor in sensitivity of data;
- retention and disposal of personal information are already linked to completion of a business purpose;
- an additional element of transparency in exception to disposal requests;
- significant new enforcement powers, potential fines and offences.

The exception for information about minors will cause operational issues for most organizations. The personal information of minors is usually treated no differently than that of adults for valid business reasons. For example, in the health insurance industry, it would be operationally impossible from a disposal request perspective to treat minor health claims data differently from adults claims data. In the telecommunications industry, several mobile phones can be on the same account and, without collecting more personal information, the telecom carrier has no way of knowing if a mobile phone is used by a minor.

We believe that the new CPPA provisions on safeguarding, retention and disposal already significantly increase the protection of minors' personal information. For example, the new category of sensitive data explicitly references information of minors, requires consideration of sensitivity of data that would include minors in setting retention periods, and introduces new enforcement powers and significant fines. That is why we recommend deleting the reference to minors from the exceptions in ss. 55(2)(d) and (f).

These concerns can be remedied with targeted changes intended to reflect what we believe to be the policy intent. Our proposed changes to the exception in s. 55(2)(f) would give sufficient flexibility for organizations while maintaining their accountability.

RECOMMENDATION:

2. **The CBA Section recommends that s. 55(2) be amended by deleting the reference to minors in (d) and (f) and introducing a new exception for already recognized reasonable business purposes.[8]**

Exception

55 (2) *An organization may refuse a request to dispose of personal information in the circumstances described in paragraph (1)(b) or (c) if*

(a) *disposing of the information would result in the disposal of personal information about another individual and the information is not severable;*

8 The black underlined and strikethrough are changes from Bill C-27 over C-11 for convenience purposes only and would be removed to show only C-27 text; actual proposed changes to C-27 are in red

> ***(b)*** *there are other requirements of this Act, of federal or provincial law or of the reasonable terms of a contract that prevent it from disposing of the information;*
>
> ***(c)*** *the information is necessary for the establishment of a legal defence or in the exercise of other legal remedies by the organization;*
>
> ***(d)*** ***~~the information is not in relation to a minor and~~*** *the disposal of the information would have an undue adverse impact on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service to the individual in question;*
>
> ***(e)*** *the request is vexatious or made in bad faith;* ***~~or~~***
>
> ***(f) retention of the information by the organization is reasonably necessary for the purposes of an activity performed under s. 18 [BA + LI], 22(2) [M&A], 24 [employment for FWUBs], 26 [witness], 27 [fraud], 40 [breach of agreement/contravention of law], 41 [investigations], 43 through 50 [disclosure to gov't institutions/required by law], and the organization informs the individual of the remaining period of time for which the information will be retained; or***
>
> ***(g)*** *the information* ***~~is not in relation to a minor and it~~*** *is scheduled to be disposed of in accordance with the organization's information retention policy, and the organization informs the individual of the remaining period of time for which the information will be retained.*

IV. PROCEDURAL AND SUBSTANTIVE FAIRNESS AT THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

The CPPA creates several roles for the OPC: an advisor to organizations (s. 110(e)); a complainant (s. 82(2)); an investigator (ss. 83-84); and an adjudicator (s. 93). Having these potentially conflicting roles reside in a single entity could create serious procedural and substantive fairness concerns for organizations and individuals. The CBA Section recommends that several safeguards be implemented to promote fairness, particularly in relation to the OPC and inquiries along with interim and final orders.

The CPPA does not adequately protect procedural fairness during either the inquiry phase or order-making. Section 90(3) gives organizations "an opportunity to be heard." More detail about those participation rights is needed. Strict segregation of duties within the OPC is also critical.

If the OPC is to have both investigative and adjudicative functions when conducting inquiries and issuing orders, rules of procedure should be created pursuant to s.92 and must:

- Embody the seven minimum requirements for procedural fairness;[9]

[9] 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;

- Establish the administrative and operational separation of functions within the OPC; and
- Be created through a public process that is iterative and open to all interested parties.

Rules of procedure for administrative bodies are challenging to draft and benefit from a variety of perspectives. When the Canadian Radio-Television and Telecommunications Commission (CRTC) revised its Rules of Procedure, it undertook informal consultations, a public CRTC proceeding and a formal regulation-making process. The draft Rules evolved significantly through the process, addressing practical and administrative law issues raised by parties.

The broad interim order making powers proposed for the OPC in s.99(1)(d) raise additional fairness concerns and merit additional safeguards.

By their nature, interim orders will be made by the OPC with an incomplete record. Interim orders can have significant impact on parties and can effectively determine the issue. Courts require moving parties to meet high standards – such as under the *RJR MacDonald Inc. v. Canada (Attorney General)*[10] test for injunctions – to exercise these powers.

RECOMMENDATIONS:

The CBA Section recommends that:

3. **The OPC's rules of procedure mandated in s. 92 should safeguard procedural fairness and be created through a transparent, consultative and iterative public process:**

   s. 92 The Commissioner must make rules through public consultation respecting the conduct of an inquiry, including the procedure and rules of evidence to be followed, and must make those rules publicly available.

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.

10

4. **The OPC's rules, policies, processes and organization should be carefully structured to minimize the risk of unfairness and conflict between the OPC's roles as advisory, investigator and adjudicator.**
5. **The OPC's rules of procedure pursuant to s. 92 should mandate a rigorous threshold for granting interim orders.**
6. **The CPPA should be amended to allow for the appeal of interim orders to the Tribunal as of right, rather than with leave as proposed in s.102(1).**

   s.102(1) A complainant or organization that is affected by an interim order made under paragraph 99(1)(d) may~~, with leave of the Tribunal,~~ appeal the order to the Tribunal.

V. PROCEDURAL AND SUBSTANTIVE FAIRNESS AT THE TRIBUNAL

The CBA Section supports the creation of the Personal Information and Data Protection Tribunal (Tribunal). The requirement for three Tribunal members to possess privacy expertise (s.6(4)) is a welcome development. However, the CBA Section recommends that the *Personal Information and Data Protection Tribunal Act* specifically mandate the creation of rules of procedure that embody requirements for procedural fairness. These rules should be created through a public process that is iterative and open to all interested parties.

VI. AUTOMATED DECISION-MAKING

The CBA Section supports the government's initiative to create a framework for the responsible use of machine learning and automated decision-making. However, these technologies are still in their infancy. The important work of addressing potential harms to individuals must be tempered with regulatory humility to ensure that legislation does not over-reach due to unwarranted or irrational fears of new technologies. The CBA Section is of the view that the CPPA goes too far.

The CPPA defines "automated decision making" as follows:[11]

> automated decision system means any technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique.

11 Section 2(1).

The term "automated decision-making" is overbroad. The technologies caught are not restricted to those that use personal information to automatically render a decision about the individual. The term also encompasses technologies that merely "assist." An Excel spreadsheet that tabulates timesheets to pay an employee is a "rules based system" that assists the employer in calculating payroll. There may be some merit to single out rules-based systems for special treatment when the employer relies exclusively on them to calculate pay in these circumstances. However, there is no obvious reason why technologies that "assist" should be given special treatment. The CPPA should focus on the use of personal information by automated decision systems that replace human judgment.

RECOMMENDATION:

7. **The CBA Section recommends that Parliament align the provisions relating to "automated decision making" with those in the recently amended Quebec *Act respecting personal information in the private sector*.[12] In Quebec, only decision-making based "exclusively" on automated processing are subject to special requirements. The CBA Section recommends following this example and removing the words "assists or" from the definition.**

VII. OPENNESS AND TRANSPARENCY – SECTION 62

The CPPA expands openness and transparency obligations for organizations, which helps individuals to better understand how organizations collect, use and disclose their personal information. Organizations are also now exposed to significant administrative monetary penaties (AMPs) for non-compliance with these expanded obligations, highlighting the need for clear language and sufficient flexibility for organizations to meet them.

Making information "readily available" is in line with evolving best practices. However, it may prove to be problematic given the new obligation in s. 62(2)(e) to make available information about retention periods applicable to sensitive personal information. If read too literally, this new obligation raises serious operational and security concerns if organizations are required to provide detailed retention periods. For example:

- **Administrative concerns:** Organizations can have hundreds of record categories. Some personal information may be in more than one category depending on the type of record and use. Record categories change over

12 CQLR c P-39, art. 12.1, as amended by An Act to modernize legislative provisions as regards the protection of personal information, SQ 2021, c 25.

time for many reasons, becoming shorter or longer (e.g. efforts to streamline the number of record categories; changes to regulatory requirements, consumer expectations and industry practice; new OPC findings) and can impact systems differently depending on whether they are legacy vs. new systems.

- **Security concerns:** Similar to security concerns on the disclosure of the actual names of third-party service providers, making readily available too much detail about record categories and specific retention periods can serve as a road map for bad actors.
- **Customer confusion:** Having to give detailed information about record categories could create customer confusion and overwhelm customers if information is given at a too granular level, particularly for organizations with complex data needs or broad product and service offerings.
- **Legal risk:** Potential for additional legal risk if an organization does not meet published retention periods (e.g. contractual, misleading or unfair practices under the *Competition Act*).

Simply adding "a general account of" to the obligation in (e) would be consistent with the obligations in s. 62(2)(b) and (c), offers some flexibility for business, avoids overwhelming consumers, and allows for establishment of best practices, including through potential codes of practice, and OPC guidance over time.

RECOMMENDATION:

8. The CBA Section recommends that s. 62(2)(e) be amended by adding the words "a general account of"

Additional information

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

(a) *a description of the type of personal information under the organization's control;*

(b) *a general account of how the organization ~~makes use of~~ uses the personal information~~, including~~ and of how ~~the organization~~ it applies the exceptions to the requirement to obtain an individual's consent under this Act, including a description of any activities referred to in subsection 18(3) in which it has a legitimate interest;*

(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 a significant impact~~s~~ 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;*

> ***(e)*** ***a general account of*** *the retention periods applicable to sensitive personal information;*
>
> ***(f)*** *how an individual may make a request for disposal under section 55 or access under section 63; and*
>
> ***(g)*** *the name or title, and business contact information of the individual to whom complaints or requests for information may be made.*

VIII. SENSITIVE PERSONAL INFORMATION

The sensitivity of personal information is a key concept in the proposed legislation and is explicitly referred to in multiple sections.[13] The sensitivity of information is also needed to determine penalties (s. 93). However, there is no contextual guidance to interpret sensitivity in the legislation.

PIPEDA and legislation in other jurisdictions have taken a principled approach to defining sensitive information.

PIPEDA explicitly requires a contextual assessment of personal information sensitivity. The OPC recently confirmed this contextual approach in an Information Bulletin on sensitive information.[14] 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.

Quebec's new legislation, *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."[15]

---

13 Sensitivity of personal information is referenced in 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)

14 OPC *Interpretation Bulletin: Sensitive Information* dated May 2022, online.

15 *An Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021, c25

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

RECOMMENDATIONS:

The CBA Section recommends that the CPPA be amended to include:

9. **a contextual assessment of the sensitivity of personal information that 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.**
10. **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.**

IX. CONCLUSION

The CBA Section reiterates its support for Bill C-27 and the CPPA and the timely passage of this important legislation. The CPPA is solid in its underlying principles and balanced in its approach. PIPEDA has served Canadians well for two decades, but privacy legislation is now in need of significant reform to meet the technological and social challenges of an evolving digital era. Domestically, CPPA demonstrates leadership in privacy, reducing the risk of fragmentation of approach across different jurisdictions. Internationally, the CPPA better aligns Canada with global trends in privacy regulation. The CBA Section's proposed amendments are targeted to enhance the effectiveness and feasibility of the bill's privacy protections, while supporting a fair process.

X. SUMMARY OF RECOMMENDATIONS

1. **The CBA Section recommends that the definition of "anonymize" be amended to be more consistent with existing case law and to balance risks of harm to individuals against achievable industry practices:**

   Anonymize means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that <u>there</u> is no <u>reasonably foreseeable risk in the circumstances</u> that an individual can be identified from the information, whether directly or indirectly, by any means. (suggested amendments underlined)

2. **The CBA Section recommends that s. 55(2) be amended by deleting the reference to minors in (d) and (f) and introducing a new exception for already recognized reasonable business purposes.**[16]

Exception

55 (2) *An organization may refuse a request to dispose of personal information in the circumstances described in paragraph (1)(b) or (c) if*

(a) *disposing of the information would result in the disposal of personal information about another individual and the information is not severable;*

(b) *there are other requirements of this Act, of federal or provincial law or of the reasonable terms of a contract that prevent it from disposing of the information;*

(c) *the information is necessary for the establishment of a legal defence or in the exercise of other legal remedies by the organization;*

(d) ***~~the information is not in relation to a minor and~~*** *the disposal of the information would have an undue adverse impact on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service to the individual in question;*

(e) *the request is vexatious or made in bad faith;* ***~~or~~***

(f) retention of the information by the organization is reasonably necessary for the purposes of an activity performed under s. 18 [BA + LI], 22(2) [M&A], 24 [employment for FWUBs], 26 [witness], 27 [fraud], 40 [breach of agreement/contravention of law], 41 [investigations], 43 through 50 [disclosure to gov't institutions/required by law], and the organization informs the individual of the remaining period of time for which the information will be retained; or

(g) *the information* ***~~is not in relation to a minor and it~~*** *is scheduled to be disposed of in accordance with the organization's information retention policy, and the organization informs the individual of the remaining period of time for which the information will be retained.*

3. **The OPC's rules of procedure mandated in s. 92 should safeguard procedural fairness and be created through a transparent, consultative and iterative public process:**

s. 92 The Commissioner must make rules <u>through public consultation</u> respecting the conduct of an inquiry, including the procedure and rules of evidence to be followed, and must make those rules publicly available.

16 The black underlined and strikethrough are changes from Bill C-27 over C-11 for convenience purposes only and would be removed to show only C-27 text; actual proposed changes to C-27 are in red

4. **The OPC's rules, policies, processes and organization should be carefully structured to minimize the risk of unfairness and conflict between the OPC's roles as advisory, investigator and adjudicator.**

5. **The OPC's rules of procedure pursuant to s. 92 should mandate a rigorous threshold for granting interim orders.**

6. **The CPPA should be amended to allow for the appeal of interim orders to the Tribunal as of right, rather than with leave as proposed in s.102(1).**

   s.102(1) A complainant or organization that is affected by an interim order made under paragraph 99(1)(d) may~~, with leave of the Tribunal,~~ appeal the order to the Tribunal.

7. **The CBA Section recommends that Parliament align the provisions relating to "automated decision making" with those in the recently amended Quebec *Act respecting personal information in the private sector*.[17] In Quebec, only decision-making based "exclusively" on automated processing are subject to special requirements. The CBA Section recommends following this example and removing the words "assists or" from the definition.**

8. **The CBA Section recommends that s. 62(2)(e) be amended by adding the words "a general account of"**

   Additional information

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

   (a) *a description of the type of personal information under the organization's control;*

   (b) *a general account of how the organization ~~makes use of~~ uses the personal information~~, including~~ and of how ~~the organization~~ it applies the exceptions to the requirement to obtain an individual's consent under this Act, including a description of any activities referred to in subsection 18(3) in which it has a legitimate interest;*

   (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 a significant impact~~s~~ on them;*

---

17 CQLR c P-39, art. 12.1, as amended by An Act to modernize legislative provisions as regards the protection of personal information, SQ 2021, c 25.

> ***(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;*
>
> ***(e) a general account of*** *the retention periods applicable to sensitive personal information;*
>
> ***(f)*** *how an individual may make a request for disposal under section 55 or access under section 63; and*
>
> ***(g)*** *the name or title, and business contact information of the individual to whom complaints or requests for information may be made.*

The CBA Section recommends that the CPPA be amended to include:

9. **A contextual assessment of the sensitivity of personal information that 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.**

10. **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.**