CBA Recommendations – Bill C-27 CPPA

October 24, 2023

The Canadian Bankers Association (CBA) is supportive of many of the key foundations of Bill C-27's Consumer Privacy Protection Act (CPPA). The CPPA requires organizations to comply with a collection of interconnected provisions that provide a solid privacy foundation based on accountability, reasonability, and proportionality. As a result, any individual CPPA provision cannot be considered solely on its own, but must be considered in combination with the Act's other supporting requirements.

A principles-based approach is highly appropriate with the CPPA's accountability model, as organizations can scale their privacy programs and processes to meet the needs associated with the sensitivity and volume of data, and leverage best practices and Privacy Commissioner guidance. The CPPA also introduces enforcement powers that will incentivize and reinforce compliance.

It is important that key concerns associated with CPPA proposals that would be new in the Canadian context are addressed before the legislation is passed into law. In particular, CPPA provisions should:

- **Avoid** situations where new transparency requirements could replicate the equivalent of **"consent fatigue" or "cookie banner fatigue"** with no meaningful value to consumers;
- **Ensure appropriate limits** so privacy rights cannot be abused or leveraged by criminals to circumvent processes designed to protect against fraud, money laundering or cyber threats;
- Ensure any requirements that are highly complex or operationally onerous would in fact **address the right underlying privacy risks and policy intent**, without negatively impacting legitimate operations, product and service delivery for consumers, or safeguarding of their personal information;
- **Harmonize** with other existing jurisdiction provisions where it makes sense; and
- **Support other policy areas** where appropriate (e.g., information sharing to support the AML regime).

As a result, we are putting forward recommendations for critical, targeted amendments in several key areas of the CPPA, after having thoughtfully considered policy intent and the impact of the CPPA to customers as well as banks and organizations of all sizes. Our key recommendations focus on:

- **Automated decision systems** – to ensure the scope of systems captured makes sense;
- **Disposal and retention** – to ensure consumers' legitimate products and services are not impacted, to reduce consumer overwhelm, to ensure appropriate risks are addressed, and to harmonize with other jurisdictions where it makes sense;
- **De-identification and anonymization** – to reduce unintended consequences that could ultimately reduce privacy protection for individuals;
- **Addressing criminal activity and intent** – to enable limited information sharing to combat money laundering and terrorist financing, and to prevent abuse of rights by criminals;
- **Consent** – a technical amendment to align to PIPEDA and provincial wording to avoid unintended consequences in scenarios involving third party consent; and
- **Implementation and enforcement** – to permit appropriate development of regulations and guidance and provide sufficient implementation runway.

APPENDIX: CBA Recommendation Detail – Bill C-27 CPPA

---

1. Automated Decision Systems: *Appropriately scope the definition of "automated decision systems" so that systems explanations are only required for systems that materially contribute to a human decision:*

2 (1) ***automated decision system*** means any technology that ~~**assists or**~~ replaces **or materially assists** 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.

Note*: This amendment addresses scenarios where an automated decision system may provide only a small input to a decision, prediction or recommendation. We also support the current CPPA wording for ss. 63(3), which requires an explanation relating to automated decision systems only if the prediction, recommendation or decision about the individual could have a "significant impact" on them. Without qualifiers in both the automated system definition as described above and in ss. 63(3), organizations may be compelled to put processes in place to provide explanations on request for almost all of their systems, without providing meaningful privacy value for consumers (e.g., if an organization has an automated online survey that recommends an ice cream flavour, or if the contribution of a system to an overall prediction, recommendation or decision is only one of 10 factors). We also note that privacy rights in other jurisdictions (e.g., Quebec, the EU) focus on exclusively automated systems, and that transparency relating to artificial intelligence systems is addressed via Bill C-27's Artificial Intelligence and Data Act.*

---

2. Disposal Requests / Retention

2.a. *Restructure disposal request exceptions relating to minors to apply only in situations where there may be a reasonable expectation that there would be residual reputational risk, so that legitimate products and services (e.g., beneficiary information, debit/credit cards that are secondary to parental cards, inputs to familial financial planning) are not adversely impacted:*

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

…

(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;

…

(f) 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.

And add:

The exceptions in (d) and (f) do not apply if the information is in relation to a minor and there is a reasonable possibility of reputational risk to the minor if the information is not deleted.

Note*: We support the continued inclusion of ss. 55(2)(f) (as amended above) as a critical provision for businesses who develop reasonable, effective and efficient retention policies and processes. Retention policies and processes are already subject to a PIPEDA/CPPA requirement for information to only be retained as long as necessary for the purposes for which it was collected, and under the CPPA, this requirement is subject to Administrative Monetary Penalties (ss. 94(1)(i)). Without this provision, other exceptions would be required to address various other valid and reasonable business purposes for retention (e.g., fraud detection or to establish, exercise or defend an ongoing, threatened or reasonably anticipated dispute, lawsuit or other proceeding, reasonable archival or backup purposes where deletion of individual records may compromise the integrity of the system, when data systems are complex and a deletion may have negative downstream consequences) and/or customer agreements (i.e., "terms of a contract" under ss. 55(2)(b)) may become very lengthy, with a potential for customer overwhelm similar to consent fatigue.*

*****

2.b. *Replace "remaining period of time for which the information will be retained" with "duration of the period of time information will be kept" to harmonize with Quebec requirements and promote a consistent customer experience:*

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

…

(f) 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**~~ **duration of the period of time information will be kept**.

*****

2.c. *Amend the new transparency requirement relating to retention periods of sensitive personal information to require only a "general account", similar to other transparency requirements, to avoid consumer overwhelm and prevent criminals from obtaining and using detailed information to target organizations with sensitive information:*

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

…

(b) a **general account** of how the organization uses the personal information…;

(c) a **general account** of the organization's use of any automated decision system…;

…

(e) **a general account of** the retention periods applicable to sensitive personal information;

---

3. De-identification / Anonymization: *The CBA supports recommendations from the Canadian Anonymization Network (CANON), including the following:*

3.a. *Modify the definition of "anonymize" to be consistent with other Canadian jurisdictions and jurisprudence by including a reasonability factor:*

2(1) ***anonymize*** means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that **there is** no **reasonably foreseeable risk in the circumstances that an** individual can be identified from the information, whether directly or indirectly, by any means.

*****

3.b. *Add an exception to the prohibition to re-identification to remove unnecessary barriers to legitimate scenarios such as when de-identification is only used for safeguarding, a customer has provided consent, or there is a basis for collection or use without knowledge or consent (e.g., re-identifying when analysis of de-identified information indicates fraud):*

75 An organization must not use information that has been de-identified, alone or in combination with other information, to identify an individual except

(a) where the organization can rely on consent or another authority under this Act to use the personal information;

…

Note: *existing subsections. 75(a)-(f) would be renamed to (b)-(g).*

---

4. AML/ATF Information Sharing: *Help organizations combat money laundering and terrorist financing by providing a legal basis for reasonable voluntary and discretionary information sharing between organizations that participate in Canada's AML/ATF regime, as part of the existing CPPA provision relating to AML disclosures:*

46 (1) An organization may disclose an individual's personal information without their knowledge or consent to the government institution referred to in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section.

(2) An organization may collect, use or disclose an individual's personal information without their knowledge or consent as permitted by a framework defined under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Note*: Done in the right way, we expect this private-to-private information sharing to* increase *privacy protections for Canadians by* reducing *unnecessary reporting to the government on low-risk transactions, and simultaneously* increasing *the effectiveness of overall*

reporting in Canada's AML regime. An amendment to the CPPA is necessary to provide a legal basis for such sharing as organizations cannot rely on the CPPA's "legitimate interests" provisions (because s. 18 does not permit disclosures). A subsequent amendment to the PCMLTFA (managed separately from Bill C-27) would set out appropriate guardrails, governance and oversight parameters for information sharing "frameworks"; a consultation by the Department of Finance involving information sharing closed in August 2023.

---

5. Prevent Abuse of Rights: *Prevent criminals from abusing privacy rights to circumvent processes designed to detect, prevent or suppress crime (e.g., fraud, money laundering, terrorist financing, cyber attacks) when an organization is required to respond to consumer requests (e.g., disposal requests, automated decision system explanations or access requests) by ensuring that organizations are not required to provide information that may contravene a law (e.g., PCMLTFA s. 8's tipping prohibition), reveal confidential commercial information, or compromise an ongoing investigation:*

Exceptions to Responding to Requests
XX Organizations are not required to provide responses, types of personal information, reasons or principal factors that may contravene a law, reveal confidential commercial information, or compromise an ongoing investigation, in responding to requests set out in sections 55, 63, or 73.

***Note**: This is drafted as a single provision to address all types of requests; an alternative approach would be to include similar language in each of sections 55, 63 and 73. Existing wording in ss.70(7) is insufficient on its own as it only addresses confidential commercial information and requests for* personal information *under s. 63.*

---

6. **Consent**: *Avoid introducing potential unintended consumer consequences and confusing consent obligations when organizations need to rely on consent obtained by another organization (e.g., background checks, data mobility requests), through a technical amendment to realign to existing PIPEDA wording and provincial approaches:*

15 (1) Unless this Act provides otherwise, ~~**an organization must obtain**~~ an individual's valid consent **is required** for the collection, use or disclosure of the individual's personal information.

---

7. **Implementation / Enforcement**:

7.a. Provide at least a two-year implementation period for most provisions, as well as a graduated or grace period for enforcement, that aligns with the timing required to develop regulations and necessary guidance with appropriate stakeholder consultation, particularly given scarcity of technology resources to execute necessary changes to systems

7.b. Provide for timely implementation for information sharing to permit selected organizations to share information to combat money laundering and terrorist financing (as in Recommendation #4).

---

8. **Additional Comments in Support of the Current Approach Under the CPPA**:

- **Authorized Representatives:** We support the current wording of s. 4 of the CPPA. Any inclusion of extending an individual's privacy rights to *any person authorized in writing* yields a significant potential for fraud, coercion, financial abuse and circumvention of other provisions that may address specific privacy considerations (e.g., data mobility frameworks), which would significantly increase risks to consumers.
- **Breach Reporting:** We support the current wording of ss. 58(2) of the CPPA. The requirement to provide a breach report to the privacy regulator *as soon as feasible after the organization determines that the breach has occurred* is reasonable as it can take time to confirm whether a breach has occurred, particularly if an organization is large or the extent of the breach is unclear (e.g., to inform the right internal group, to determine whether personal information was impacted, to perform a risk assessment, to gather even basic information for the breach report, etc.). In addition, notification of the regulator should not distract from the organization's ability to contain and address the breach itself.
- **Legislating Best Practices:** The prescriptive use of best practices should not be set out in legislation, but left to guidance. PIPEDA and CPPA are both primarily principles-based and require a proportionate approach. Many organizations, like banks, already scale their privacy approach to the sensitivity and nature of the data and the specific circumstances, and enforcement measures introduced in the CPPA will only further incentivize and reinforce compliance. Mandating formal approaches such as privacy-by-design, privacy impact assessments or use of specific techniques or technologies in the legislation itself is unnecessary.