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** –

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.

55(2)