PRIVACY REFORM IS ON THE TABLE ONCE MORE: CANADA INTRODUCES THE *DIGITAL CHARTER IMPLEMENTATION ACT, 2022*

Posted on June 22, 2022

Categories: Insights, Publications

Once again, Canada has taken a step forward in its journey toward strengthening its privacy and data protection laws in a manner consistent with global trends.

On June 16, 2022, the Federal Government tabled Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts,*[1] *known by its short title as the Digital Charter Implementation Act, 2022* ("**Bill C-27**"). If passed, Bill C-27 will materially change the legal landscape for privacy and data protection in Canada.

In particular, Bill C-27 would substantially amend the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("**PIPEDA**"), to remove the provisions governing handling of personal information ("PI"), and it would enact the *Consumer Privacy Protection Act* (the "**CPPA**"), the *Artificial Intelligence and Data Act* (the "**AIDA**"), and the *Personal Information and Data Protection Tribunal Act* ("**PIDPTA**") that will establish a Personal Information and Data Protection Tribunal (the "**Tribunal**").

The proposed CPPA and PIDPTA include a number of elements that were first proposed in November 2020 pursuant to Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts* ("**Bill C-11**"), which died on the Order Paper in 2021 as a result of the Federal election. However, Bill C-27 also includes additional reforms, including the proposed AIDA.

Everything old is new again

The proposed CPPA pursuant to Bill C-27 carries the same name as the new Federal data protection legislation that was proposed pursuant to Bill C-11, and many of the terms are very similar to those proposed under Bill C-11 (see our article on Bill C-11 for more information). Some of the key elements that expand upon existing PIPEDA requirements and are still included in the currently proposed CPPA include the following:

- Every organization will be required to have a **Privacy Management Program**, including addressing protection of PI, handling complaints and requests for information, staff training, and developing materials to explain the organization's policies and procedures.[2]
- Codification of the "**Appropriate Purpose Test**", which has long been applied by privacy regulators, labor arbitrators and other adjudicators to assess whether a reasonable person would consider the purpose for collecting, using and/or disclosing (collectively "**Processing**" and similar terms will have commensurate meanings) PI to be appropriate in the circumstances.[3] Relevant factors will include the sensitivity of the PI, the legitimate business needs of the organization, the effectiveness of the organization's Processing of PI to meet such needs, whether there is a less invasive option (at comparable cost and with comparable benefits), and whether the loss of privacy would be proportionate to the benefits gained.[4]
- New **conditions for valid consent**, including a requirement for certain specified information to be provided to individuals in "plain language" before or at the time when consent is sought.[5] Similarly to the Office of the Privacy Commissioner of Canada's current "Guidelines for obtaining meaningful consent",[6] individuals would need to be provided with details regarding the purposes for Processing their PI, the manner in which PI is Processed, the type(s) of PI that will be Processed, the third parties that PI may be disclosed to, and any reasonably foreseeable consequences.
- New **exceptions to consent** for certain socially beneficial purposes (if the PI is de-identified),[7] or where the PI is collected or used for certain business activities – i.e., activities that are necessary to provide a product or service to the individual, for IT security, or for the safety or security of a product or service.[8] However, the collection or use of PI for business activities must be within the reasonable expectations of the individual, and the PI must not be collected or used for the purpose of influencing the individual's behaviour or decisions.
- Clearly **limiting the obligations of service providers**, such that they will only be subject to the safeguarding requirements and an obligation to notify the data controller of a breach of such safeguards, unless the service provider Processes the PI for its own purposes (i.e., not just the purposes for which the controlling organization transferred it to the service provider).[9] Similarly to current PIPEDA requirements, the CPPA provides that organizations must use contractual or other measures to ensure that their service providers will protect the PI that they process.[10]
- Additional transparency requirements, including (without limitation) with respect to **cross-border transfers of PI & automated decision systems**.[11]
- New **data subject rights**, including a right to data deletion that allows individuals to request disposal of their information (subject to certain limitations and exceptions),[12] as well as certain data mobility rights (i.e., where the relevant organizations are subject to a data mobility framework).[13]
- Materially **enhanced enforcement mechanisms**, including administrative monetary penalties ("**AMPs**")

up to the greater of $10,000,000 or 3% of the organization's gross global revenue in its prior financial year,[14] penalties for certain offences up to the greater of $25,000,000 or 5% of the organization's gross global revenue in its prior financial year,[15] and a private right of action for individuals affected by an organization's contravention of the CPPA.[16]

Despite lobbying efforts by the Office of the Privacy Commissioner of Canada ("**OPC**") since the CPPA was first proposed in 2020, Bill C-27 still would not grant the OPC the power to impose AMPs or levy fines for offences under the CPPA. However, the OPC will have the power to make compliance orders, audit the PI management processes of organizations, and recommend that an AMP be imposed by the Tribunal on organizations that contravene certain provisions of the CPPA. The Tribunal may then impose a penalty on the organization, if it deems appropriate, after providing the organization and the OPC with an opportunity to make representations. Pursuant to the PIDPTA, the Tribunal will also handle appeals of certain findings, orders and decisions under the CPPA.[17]

New and Notable

Although Bill C-27 contains a number of provisions that are similar to those that were proposed pursuant to Bill C-11, it also introduces the AIDA as well as some added requirements and restrictions under the CPPA.

The Artificial Intelligence and Data Act

A notable addition to Bill C-27 is the proposed creation of AIDA, which is intended to regulate international and interprovincial trade and commerce in artificial intelligence systems[18] ("**AI Systems**") by establishing common requirements across Canada for such systems, and to prohibit certain conduct in relation to AI Systems that may result in serious harm to individuals or their interests.

More particularly, the AIDA imposes a number of requirements and restrictions with respect to the following regulated activities when they are carried out in the course of international or interprovincial trade and commerce:

- processing or making available for use any data relating to human activities for the purpose of designing, developing or using an AI System; and/or
- designing, developing or making available for use an AI System or managing its operations.

A person that carries out a regulated activity involving processing (or making available for use) anonymized data, must establish measures with respect to the manner of anonymizing data and the use or management of anonymized data.[19] In addition, the AIDA sets out record keeping obligations applicable to persons that carry out regulated activities, and requires such persons to assess whether the AI System is a "high-impact system" (the criteria for which will be prescribed by regulation). Additional obligations will apply to persons that

make available for use (or manage the operation of) "high-impact systems", including requirements to:

- establish measures to identify, assess and mitigate the risks of **harm**[20] or **biased output** that could result from the use of the system;
- establish measures to monitor compliance with the mitigation measures, and the effectiveness of those mitigation measures; and
- publish on a publicly available website a plain-language description of the system, including an explanation of how the system is intended to be used, the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make, the established mitigation measures (as described above), and any other prescribed information.

For the purposes of the AIDA, "biased output" means content that is generated, or a decision, recommendation or prediction that is made, by an AI System, which adversely differentiates, (directly or indirectly), without justification, in relation to an individual based on the prohibited grounds of discrimination under section 3 of the *Canadian Human Rights Act*.[21] However, this will not include content, or a decision, recommendation or prediction, the purpose and effect of which are to prevent, reduce or eliminate disadvantages suffered by any group of individuals when those disadvantages are based on, or related to, the prohibited grounds of discrimination.

In addition, the person responsible for a high impact system must notify the Minister[22] if the use of the system results (or is likely to result) in material harm. The Minister will have broad powers, including the ability to require that any person who is responsible for a high-impact system must cease using it or making it available for use if the Minister has reasonable grounds to believe that it gives rise to a serious risk of imminent harm.

Importantly, pursuant to the AIDA, it will be an offence for any person to:[23]

- Possess or use PI for the purpose of designing, developing, using or making available for use an AI system, if the person knows or believes that the PI was obtained or derived, directly or indirectly, as a result of the commission of an offence under any Act of Parliament or a provincial legislature (or an act or omission anywhere that, if it had occurred in Canada, would have constituted such an offence);
- Without lawful excuse, knowingly or recklessly make an AI System available for use, which is likely to cause serious physical or psychological harm to an individual or substantial damage to an individual's property, if the use of the system causes such harm or damage; or
- Make an AI System available for use, with intent to defraud the public and to cause substantial economic loss to an individual, if the use of such system causes that loss.

Like the CPPA, the AIDA also includes significant enforcement mechanisms, including providing for AMPs for contraventions of the AIDA,[24] as well as penalties of up to the greater of $25,000,000 or 5% of the organization's gross global revenue in its prior financial year for the indictable offences, noted above, committed by organizations.[25]

Additions to the CPPA

(1) Greater specificity regarding anonymized and de-identified PI

Bill C-27 clearly distinguishes between 'de-identified' information and 'anonymized' information. 'De-identified information' does not allow an individual to be directly identified, but still carries a risk that the individual may be identified. 'Anonymized information' is PI that has been irreversibly and permanently modified 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.

Bill C-27 provides that the CPPA will not apply to PI that has been anonymized,[26] and that anonymizing information is equivalent to disposing of it for the purposes of the CPPA.[27] On the other hand, de-identified information will continue to be considered PI for most purposes under the CPPA.[28] However, the knowledge and consent of the relevant individual(s) will not be required for an organization to use PI in order to de-identify it.

(2) New consent exceptions, including for "legitimate interests"

The proposed CPPA includes new exceptions to the general requirement for consent to Process PI. In particular, similarly to the well-known General Data Protection Regulation that applies to processing of personal data in the European Economic Area ("**EEA**"), under the proposed CPPA an organization could collect and use PI without an individual's knowledge or consent for an activity in which the organization has a "legitimate interest" that outweighs any potential adverse effect on the individual. However, certain limitations and conditions will apply, including as follows:[29]

- The collection or use of the PI must be something that a reasonable person would expect for the organization's activity;
- The PI must not be collected or used for the purpose of influencing an individual's behaviour or decisions; and
- Prior to collecting or using the PI, the organization must identify potential adverse effects and take reasonable measures to reduce the likelihood of such effects (or mitigate or eliminate such effects).

Although this new exemption to consent requirements is potentially helpful to organizations, the restriction upon relying on "legitimate interests" for purposes that involve influencing behaviours and decisions

constitutes a significant restraint. In particular, this would appear to limit the ability of organizations to rely on this exemption for marketing activities (including for targeted advertising purposes).

(3) Same teeth, wider mouth?

As noted above, Bill C-27 provides for significant AMPs and fines under the CPPA, with maximum penalties that mirror those previously proposed under Bill C-11. However, under Bill C-27, AMPs can be imposed for a broader range of potential contraventions of the CPPA, including for non-compliance with the privacy management program requirements under section 9(1), failure to ensure that a service provider will protect PI pursuant to section 11(1), failure to specify the purposes for Processing PI under sections 12(3)-(4), failure to respond appropriately to a withdrawal of consent, and/or failure to obtain consent in accordance with the CPPA.

Conclusion

Some aspects of Bill C-27 are likely to be welcomed by organizations, including the enhanced clarity regarding obligations of service providers versus organizations that "control" PI, as well as the new exemptions from potentially onerous and unrealistic consent requirements. However, the CPPA will be stricter and more proscriptive than PIPEDA in a number of respects. Accordingly, if the legislation passes, it will be important for organizations to review and update their privacy and data protection compliance programs.

Although Bill C-27 has only recently been introduced, and may still be amended as it works its way through the legislative process, there is significant impetus for statutory reform (including to ensure Canada's continuing "adequacy" status for transfers of personal data from the EEA to Canada). Given the material penalties for non-compliance that are proposed under Bill C-27, organizations that may be subject to the CPPA or AIDA should begin preparing for the likely statutory changes, so that they will be well-positioned to comply if/when such changes pass and come into force. In the interim, McMillan's Privacy & Data Protection Group will continue to monitor the proposed legislation closely, and to provide updates on its progress.

McMillan Vantage, McMillan LLP's public affairs arm, can also assist organizations that wish to engage with the Federal government to advocate for changes to the proposed legislation, or to assist with communicating the pending statutory requirements within the organization.

[1] Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts,* 1st Sess, 44th Parl, 2022.
[2] Proposed CPPA, section 9(1).
[3] Proposed CPPA, section 12(1).
[4] Proposed CPPA, section 12(2).

[5] Proposed CPPA, sections 15(3)-(4).
[6] Office of the Privacy Commissioner of Canada "Guidelines for Obtaining Meaningful Consent" (2018 May; last revised 2021 August 13), online: Office of the Privacy Commissioner of Canada.
[7] Proposed CPPA, section 39.
[8] Proposed CPPA, section 18.
[9] Proposed CPPA, section 11(2).
[10] Proposed CPPA, section 11.
[11] Proposed CPPA, section 62.
[12] Proposed CPPA, section 55.
[13] Proposed CPPA, section 72.
[14] Proposed CPPA, section 95(4).
[15] Proposed CPPA, section 128.
[16] Proposed CPPA, section 107.
[17] Proposed PIDPTA, section 5.
[18] Defined as: "a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions."
[19] Proposed AIDA, section 6.
[20] For this purpose, "harm" includes physical or psychological harm, damage to property, or economic loss to an individual.
[21] The prohibited grounds are currently as follows: race, national or ethnic origin, colour, religion, age, sex (including pregnancy or child-birth), sexual orientation, gender identity or expression, marital status, family status, genetic characteristics (including refusal of a request to undergo a genetic test or to disclose, or authorize the disclosure of, the results of a genetic test), disability and conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered.
[22] The Minister is "the member of the Queen's Privy Council for Canada designated under section 31 or, if no member is so designated, the Minister of Industry".
[23] Proposed AIDA, sections 38-39.
[24] Proposed AIDA, section 30.
[25] Proposed AIDA, section 40.
[26] Proposed CPPA, section 6(5).
[27] Proposed CPPA, section 2(1), s.v. "Dispose".
[28] Proposed CPPA, section 2(3).
[29] Proposed CPPA, section 18.

by Lyndsay Wasser, Kristen Pennington, Robbie Grant, Kristen Shaw

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.