ANOTHER LEAP FORWARD FOR CANADIAN PRIVACY LAWS

Posted on November 19, 2020

Categories: Insights, Publications

On November 17, 2020, Minister Navdeep Bains presented 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*, short titled as the *Digital Charter Implementation Act, 2020* (the "**Act**"), for its first reading in the House of Commons. If passed, the Act will result in radical changes to Canada's Federal private-sector data protection legislation.

Privacy advocates will likely laud this new development. In recent years there have been numerous reports of serious privacy issues associated with collection, use, protection and disclosure of sensitive information related to large populations of individuals. The proposed statutory changes will, among other things, provide for substantial penalties if organizations do not handle personal information in accordance with the amended laws.

The Act overhauls the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), by essentially cutting it into two pieces. PIPEDA is preserved as the "*Electronic Documents Act*" and PIPEDA's provisions related to consumer privacy protection are reformed into the *Consumer Privacy Protection Act* ("**CPPA**"). The substantive law in much of the CPPA remains very similar to many of the existing PIPEDA requirements, especially with respect to matters such as: accountability; openness; limiting collection, use, disclosure and retention; accuracy; and individual access.

However, the Act will require a number of significant changes to Canadian organizations' handling of personal information, including the key differences that we have highlighted below.

1. **Privacy Management Programs**. PIPEDA requires that organizations implement policies and practices to give effect to the principles set out in Schedule 1 (including certain procedures and training requirements). However, under the CPPA there is a specific obligation for every organization to have a "privacy management program" that incorporates its policies, practices and procedures for compliance with the CPPA, including how the organization protects personal information, how it handles requests or complaints, how it trains staff, and how it develops materials to explain its policies and procedures.[1] Upon request, an organization must provide the Office of the Privacy Commissioner of Canada (the "OPC") with access to such policies, practices and procedures.[2]

2. **Appropriate Purpose Test is Expanded**. Under PIPEDA, organizations may only collect, use or disclose personal information for a purpose that a reasonable person would consider appropriate in the circumstances.[3] The CPPA draws on prior reports by the OPC and enumerates five factors relevant to this analysis: (a) the sensitivity of the information; (b) the legitimate business needs of the organization; (c) the effectiveness of the collection, use or disclosure of the information for achieving those business needs; (d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and (e) whether the individual's loss of privacy is proportionate to the benefits in light of the organization's protective measures for the personal information.[4]
3. **New Conditions for Valid Consent**. PIPEDA provides that the consent of an individual is only valid if it is reasonable to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of their personal information.[5] The CPPA goes a step further, to also set out certain information that must be provided to individuals in "plain language" at or before the time that consent is sought.[6] Again, the legislation appears to draw from prior reports and guidance from the OPC, including the "Guidelines for obtaining meaningful consent"[7] that were released in 2018.
4. **Exceptions to Consent**. PIPEDA is a consent-based statute, which only contains a few narrow exceptions to the strict consent requirements. However, the CPPA provides that an individual's knowledge and consent is not required to collect or use personal information for certain "business activities", provided that a reasonable person would expect the collection or use for that activity and the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions. The relevant business activities include, amongst others, activities that are necessary to provide / deliver a product or service that the individual has requested from the organization.[8]
5. **Socially Beneficial Purposes**. Like PIPEDA, the CPPA also sets out some other exceptions to consent requirements, including for disclosures in connection with certain investigations,[9] to government institutions for purposes such as law enforcement or public defense,[10] and otherwise as required by law.[11] However, the new legislation also includes new public interest exceptions to consent, where disclosure is for a "socially beneficial purpose" (i.e., a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose). More particularly, an organization may disclose an individual's personal information without consent if: (a) the personal information is de-identified before disclosure; (b) the disclosure is made to certain reputable institutions, such as government institutions, health care institutions, post-secondary education institutions or public libraries; and (c) the disclosure is made for a "socially beneficial purpose."[12]
6. **Transparency, Cross-Border Transfers & Automated Decision Making**. Under the CPPA, an organization must make information available regarding how it fulfills its CPPA obligations.[13] This

includes whether or not the organization transfers personal information across national borders, which, again, appears to be consistent with prior guidance from the OPC. The CPPA also directly addresses transparency related to automated decision making. Pursuant to the new legislation, organizations would be required to make available a general account of their use of certain automated decision making systems. In addition, if an automated decision making system is used to make a decision, recommendation or prediction about an individual, on request, the organization must provide that individual with an explanation of such prediction, recommendation or decision (and of how the personal information used in that process was obtained).

7. **The Right to Data Deletion**. The CPPA includes a new mechanism for individuals to request the disposal of their personal information. As in PIPEDA, organizations must dispose of information when it no longer serves its purpose.[14] Under the CPPA, they must also dispose of an individual's information upon request (subject to certain exceptions). The organization must also inform service providers of the disposal request, and seek confirmation of disposal.[15]
8. **Responsibility for Service Providers**. When it comes to service providers, the CPPA puts the primary responsibility on the organization that decides to collect the relevant information. Though the organization may transfer personal information to a service provider without additional consent,[16] the transferring organization will be accountable for the information, as long as that information is considered 'under its control'.[17] The organization must ensure (contractually or otherwise) that the service provider has substantially the same protections in place for the information, as compared to those required of the organization for the personal information in its possession.[18]
9. **Limits on Service Providers' Obligations**. Unlike PIPEDA, the CPPA clearly limits the obligations of service providers. The primary obligations under the CPPA that would apply to service providers are to: (i) protect the personal information by implementing safeguards proportionate to the information's sensitivity, and (ii) notify the controlling organization as soon as feasible if the service provider experiences a data breach.[19] However, if the service provider collects, uses or discloses the information for any purposes beyond the purpose for which it was transferred by the controlling organization, the service provider must then abide by the CPPA in its entirety.[20]
10. **A New Tribunal**. The Act creates the *Personal Information and Data Protection Tribunal Act* ("**PIDPTA**"), which establishes the Personal Information and Data Protection Tribunal (the "**Tribunal**"). This Tribunal is established for appeals from the CPPA, and may impose penalties for contraventions, as recommended by the OPC.[21]
11. **Enforcement Power**. Under PIPEDA, the OPC can only make non-binding recommendations and only certain offences can give rise to fines (up to a maximum of $100,000). The CPPA now provides for significant penalties of up to the greater of $10,000,000 or 3% of the organization's gross global revenue

in its prior financial year,[22] or for some offences up to the greater of $25,000,000 or 5% of the organization's gross global revenue.

12. **Private Right of Action**. The CPPA also creates a private right of action for individuals affected by an organization's contravention of the legislation, after the OPC has found that such a contravention has occurred. Under PIPEDA, this statutory right to seek damages is only granted to a complainant,[23] but under the CPPA any individual affected by a contravention of the CPPA has a cause of action against the organization for damages suffered by the individual as a result of the contravention.[24]
13. **Data Mobility**. Organizations will be required to transfer the personal information they have collected from an individual to another organization, upon request of the individual, in certain circumstances.[25] The CPPA contemplates that the regulations will set out this data mobility framework.

The CPPA includes some potentially beneficial changes to the federal, private-sector privacy law. In particular, the exceptions to consent for certain business activities and limited application of the requirements to service providers are likely to be helpful to Canadian businesses. However, the CPPA would have the strongest fines among G7 privacy laws,[26] and the new private right of action may give rise to an increase in privacy-related class action litigation. Accordingly, every organization that may be subject to the CPPA should begin reviewing its privacy compliance program now, in order to ensure that it is well-positioned to comply with the new legislation if/when the statutory changes come into force.

McMillan Vantage, McMillan LLP's public affairs arm, is also available to 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.

by Lyndsay Wasser and Robbie Grant

[1][ps2id id='1' target='/] CPPA, Section 9 (1)
[2][ps2id id='2' target='/] CPPA, Section 10
[3][ps2id id='3' target='/] PIPEDA, Section 5 (3)
[4][ps2id id='4' target='/] CPPA, Section 12 (2)
[5][ps2id id='5' target='/] PIPEDA, Section 6.1
[6][ps2id id='6' target='/] CPPA, Section 15(3)
[7][ps2id id='7' target='/] See: Guidelines for obtaining meaningful consent
[8][ps2id id='8' target='/] CPPA, Section 18
[9][ps2id id='9' target='/] CPPA, Sections 40-42
[10][ps2id id='10' target='/] CPPA, Sections 43-48
[11][ps2id id='11' target='/] CPPA, Sections 49-50

[12][ps2id id='12' target='/] CPPA, Section 39
[13][ps2id id='13' target='/] CPPA, Section 62
[14][ps2id id='14' target='/] PIPEDA, Schedule 1, Section 4.5.3; CPPA, Section 53
[15][ps2id id='15' target='/] CPPA, Section 55
[16][ps2id id='16' target='/] CPPA, Section 19
[17][ps2id id='17' target='/]CPPA, Section 7
[18][ps2id id='18' target='/] CPPA, Section 11
[19][ps2id id='19' target='/] CPPA, Section 61
[20][ps2id id='20' target='/] CPPA, Section 11 (2)
[21][ps2id id='21' target='/] PIDPTA, Section 5
[22][ps2id id='22' target='/] CPPA, Section 94
[23][ps2id id='23' target='/] PIPEDA, Section 16 (d)
[24][ps2id id='24' target='/] CPPA, Section 106
[25][ps2id id='25' target='/] CPPA, Section 72
[26][ps2id id='26' target='/] New proposed law to better protect Canadians' privacy and increase their control over their data and personal information

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.