Consumer Privacy Protection Act (CPPA): Increasing Accountability And Transparency

In a recent MT Cybersecurity Blog, we discussed Bill C-11, the *Consumer Privacy Protection Act* (the "**CPPA**"), which was introduced on November 17, 2020, by the Minister of Innovation, Science and Industry with the aim of modernizing federal privacy law and making it more transparent for Canadians. To keep you informed, the MT Cybersecurity Blog has published a series of articles summarizing key provisions of the CPPA and how these tentative changes may impact you.

This article will discuss the CPPA's requirements for accountability and transparency in handling personal information and developing policies and procedures. Generally, the CPPA adopts many principles already included in the *Personal Information Protection and Electronic Documents Act* (Canada) ("**PIPEDA**") while providing more robust protection to Canadians.

Accountability and Control

The CPPA's accountability provisions expand upon the Accountability Principles contained in Schedule 1 of PIPEDA. For instance, the CPPA stipulates that an organization is accountable for personal information that is under its control, which is very similar to what was already required under PIPEDA.[1] However, the CPPA takes this a step further and provides greater clarity by specifically defining "control" to mean personal information that comes under the control of the organization which decides to collect it and which determines the purposes for its collection, use or disclosure.[2] The CPPA explicitly states that the personal information will be deemed to be under an organization's control, irrespective of whether it was collected, used or disclosed by the organization itself, or by a service provider on behalf of the organization.[3] By codifying this concept, the CPPA puts greater emphasis on keeping the organization accountable to individuals.

Like PIPEDA, the CPPA also requires that an organization designate at least one individual to be responsible for the organization's compliance with its statutory privacy obligations.[4] It is important to note, however, that the CPPA has explicitly indicated that designating such an individual does not relieve an organization of its obligations under the legislation.[5] Rather, the organization itself will remain ultimately accountable for meeting the requirements of the

CPPA. Both pieces of legislation require the individual's contact information to be disclosed upon request, though from a best practices perspective, many organizations have already been including an email address or telephone number in their privacy policies that can be used in connection with any questions related to privacy protection.

Privacy Management Programs and Transparency

Both PIPEDA and the CPPA include requirements for an organization to implement policies and procedures related to certain practices of the organization. The CPPA refers to the policies and procedures as a privacy management program.[6] The requirements for a privacy management program under the CPPA and the policies and procedures under PIPEDA are almost identical. In each case, the program/procedures must cover: how personal information will be protected, how requests for information and complaints will be dealt with, how the organization will meet its other obligations under the legislation, and what training and information will be provided to the organization's staff on the foregoing.[7] Additionally, organizations must develop materials to explain their policies and procedures.

The CPPA establishes a requirement for organizations to take into account the volume and sensitivity of the personal information under its control when developing its privacy management program.[8] This suggests there is no 'one-size-fits-all' approach to privacy management programs. Instead, an organization's program will depend on the nature of the information collected, with organizations that collect large volumes of sensitive personal information, for example, medical or financial information, needing to have more robust privacy management programs in place to ensure that the information is not subject to unauthorized access or unauthorized disclosure. While the Office of the Privacy Commissioner of Canada (the "**OPC**") has stipulated in its guidelines that organizations should take into account the amount and sensitivity of the personal information collected when structuring their policies, this is not currently an express requirement under PIPEDA.[9]

Similar to the Openness Principles under PIPEDA, the CPPA requires that organizations make information explaining their policies and practices "readily available, in plain language."[10] This essentially amounts to the requirement to have a written privacy policy that is publicly available, easily accessible, and in language that the average individual can understand. In order to fulfill this obligation, an organization is required to make available a description of the type of personal information under its control and how that personal information is utilized, including how the various consent exceptions are applied.[11] Additionally, organizations must disclose the business contact information of the individual responsible for handling inquiries and complaints.[12]

OPC guidelines have recommended that organizations be transparent about their handling of personal information, specifically with regard to the transfer of personal information, but these guidelines are not currently an express requirement under PIPEDA.[13] A notable addition to the information that must be included in a privacy policy under the CPPA includes whether an organization carries on "any international or interprovincial transfer or disclosure of personal information."[14] However, this information only needs to be made available where the international or interprovincial transfer or disclosure of

personal information could have reasonably foreseeable privacy implications. The CPPA in its current draft does not provide guidance on this exception. Therefore, given the current wording of the CPPA, it is recommended that organizations err on the side of caution by disclosing whenever personal information is, or has the potential to be, transferred over a provincial or international border.

Additionally, the CPPA will require organizations that utilize automated decision systems to disclose how they use such systems "to make predictions, recommendations or decisions about individuals that could have significant impacts on them."[15] This is a new requirement that is not included in PIPEDA. Organizations will also be required to provide individuals with information regarding how they can request the disposal of, or access to, their personal information.[16]

Record Keeping and Right to Access by Commissioner

PIPEDA currently requires that organizations identify and document the purposes for which information is collected, but the CPPA takes this a step further. Organizations will be required to ascertain and record the purposes for which information is being collected, used or disclosed, at or before the time of collection. Where an organization decides that information under its control is to be used or disclosed for a new purpose, it will also need to record that new purpose prior to using or disclosing the information for the new purpose.[17]

The CPPA will also require organizations to provide the Privacy Commissioner with access to its policies, practices and procedures, upon request.[18] This is an entirely new requirement that does not exist under PIPEDA. This is only one of many proposed changes that would provide the Privacy Commissioner with greater oversight of private organizations and allow it to play a larger regulatory role.

It is important that private sector organizations familiarize themselves with the CPPA, to ensure they properly amend their policies and practices in accordance with these changes. Miller Thomson's privacy and technology experts are happy to discuss how these changes may affect your organization and how you can prepare for the CPPA, which is currently in its Second Reading.

Footnotes

1. CPPA, s. 7(1); PIPEDA, Schedule 1, Section 4.1.
2. CCPA, s. 7(2).
3. *Ibid*, s. 7(2).
4. *Ibid*, s. 8(1).
5. *Ibid*, s. 8(2).
6. *Ibid*, s. 9(1).
7. CPPA, s. 9(1)(a)-(c) and PIPEDA, Schedule 1, Section 4.1.4.
8. CPPA, s. 9(2).
9. OPC guidelines, online

10. CPPA, s. 62(1).

11. *Ibid*, s. 62(2)(a)-(b).

12. *Ibid*, s. 62(2)(f).

13. OPC guidelines, online

14. CPPA, *supra* note 2, s. 62(2)(d).

15. *Ibid*, s. 62(2)(c).

16. *Ibid*, s. 62(2)(e).

17. *Ibid*, s. 12(3) and 12(4).

18. *Ibid.,* s. 10.

by Jaclyne Reive and Kristin Dosen
Miller Thomson LLP