Goodmans LLP Update

Federal Privacy Regulation 2.0: Now with Bite and Bark

This week, the Canadian Federal Minister of Innovation, Science and Industry introduced for first reading in Parliament 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* (the "**Bill**"). Unlike the current federal private sector privacy regime, the Bill includes real teeth, so there will be important consequences for non-compliance. Also, the Bill includes new and potentially onerous regulatory requirements.

If passed into law, the Bill would: (a) amend and replace the *Personal Information Protection and Electronic Documents Act* ("***PIPEDA***") with a new *Consumer Privacy Protection Act* ("***CPPA***"), and (b) enact the *Personal Information and Data Protection Tribunal Act*, including the establishment of a new Information and Data Protection Tribunal (the "**Tribunal**") that will be empowered to hear appeals of decisions of the Privacy Commissioner of Canada ("**Commissioner**") and impose penalties under the *CPPA*.

The CPPA's Bite

The *CPPA*, like *PIPEDA*, generally permits organizations to use, collect and disclose personal information of an individual, on a limited basis, where the individual provides valid consent. Most of its core provisions mirror *PIPEDA*, as currently interpreted in guidance issued by the Commissioner and many best practices. However, in a radically different approach to *PIPEDA's* ombudsman model, where the Commissioner has no power to make binding orders, the *CPPA* empowers the Commissioner to order an organization to:

(a) take measures to comply with the *CPPA;*
(b) stop doing something that contravenes the *CPPA;*
(c) comply with the terms of a compliance agreement that has been entered into by the organization; or
(d) make public measures taken or proposed to be taken to correct the policies, practices or procedures the organization has put in place to fulfil its obligations under the *CPPA.*

The cost and disruption to an organization of implementing such orders may be considerable. While an appeal to the Tribunal from such orders is available, the legislated standard of review is such that in many instances the Commissioner will have the last word on compliance measures to be taken by an organization.

Also, if an organization has contravened certain of the key requirements of the *CPPA*, the Commissioner may recommend that the Tribunal impose a financial penalty on the organization. This penalty is capped at "the higher of $10,000,000 and 3% of the organization's gross global revenue in its financial year before the one in which the penalty is imposed". In addition, for the most serious offences, the Bill proposes "the strongest fines among G7 privacy laws – with fines of up to 5% of revenue or $25 million, whichever is greater"[1] upon prosecution. The *CPPA* also creates a private right of action against non-compliant organizations, making *CPPA*-based class actions possible, but that right is circumscribed.

[1] Innovation, Science and Economic Development Canada, News Release: *New proposed law to better protect Canadians' privacy and increase their control over their data and personal information*, November 17, 2020.

Authors

Peter Ruby
pruby@goodmans.ca
416.597.4184

Monique McAlister
mmcalister@goodmans.ca
416.597.4225

Jesse-Ross Cohen
jcohen@goodmans.ca
416.849.6903

Meghan King
mking@goodmans.ca
416.597.4164

The authors would like to thank Emma Baumann, Articling Student-At-Law for her assistance in preparing this Update.

These "teeth" change the risk management profile of privacy matters falling within the scope of the *CPPA* and likely how many organizations will deal with Canadian privacy issues.

The New Regulatory Bark

The *CPPA* contains a requirement that every organization that collects, uses or discloses personal information about individuals in the course of its commercial activities must establish a "privacy management program" that includes the organization's policies, practices and procedures implemented to fulfil its obligations under the *CPPA*. The program must have regard to the volume and sensitivity of the personal information under the organization's control. Alone, this would not be a major development as many organizations that deal with voluminous or sensitive personal information already have such a program.

What is new is that the *CPPA* grants the Commissioner the power to access and, effectively, regulate an organization's privacy management program. The scope of the Commissioner's mandate to proactively investigate privacy management programs, in the absence of a consumer complaint, is not constrained by the *CPPA*. When combined with the Commissioner's order-making power, this regime creates a potentially onerous regulatory exercise for many organizations. An organization will need to document how exactly it will comply with the *CPPA*, knowing that the Commissioner can, at any time, access that documentation and order the organization to fix anything the Commissioner finds is out of compliance. The Tribunal's power to impose a penalty does not extend to a privacy management program alone not being compliant, but the Commissioner's investigation into the program may reveal other contraventions that do attract penalties (for example, failure to protect personal information through proportionate physical, organizational and technological safeguards).

Another *CPPA* regulatory "bark" is the added requirement that personal information may be shared between parties negotiating a transaction for the purposes of due diligence *only* if that information is de-identified before it is used or disclosed and remains so until the transaction is completed. In certain transactions, this may be an important change from current practices, whereby data is usually simply protected under a non-disclosure agreement that contains the elements required under statute.

The *CPPA* also provides individuals with at least three completely new privacy rights under Canadian law:

- a right of algorithmic transparency, whereby individuals whose personal information is subject to an automated decision system (such as predictive analytics and machine learning) may require the organization to provide an explanation of the automated decision and how the personal information was obtained;
- a right of disposal, whereby individuals may request an organization dispose of all information it has collected from the individual; and
- a right to data mobility, whereby individuals would have the right to direct the transfer of their personal information from one organization to another.

Next Steps

The Bill still has to go through the legislative process. We expect it to be the subject of consultation, Parliamentary committee analysis and, perhaps, alteration before being passed into law. For this reason, we have focussed in this Update on only a small number of aspects of the proposed *CPPA*. However, there are a multitude of changes being proposed for Canada's privacy law regime, some of which may be important for particular industries and businesses. With privacy-related legislative efforts underway in Quebec, Ontario, British Columbia and now federally, this is a subject to watch in the months ahead.

For more information, please contact any member of our Privacy Law Group.