David Young Law
Compliance Bulletin

November 2020

New federal privacy law – a fine balance between the GDPR and PIPEDA?

On Tuesday, November 17 the federal government introduced its long-awaited legislation to reform Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). By Bill C–11, the *Digital Charter Implementation Act*, the government proposes to replace PIPEDA with a new act, the *Consumer Privacy Protection Act* ("CPPA"), and to enact a separate law, the *Personal Information and Data Protection Tribunal Act,* to create a quasi-judicial tribunal to impose monetary penalties and rule on appeals from orders and related matters determined by the federal Privacy Commissioner under the CPPA.

There has been pressure from many quarters – including the Privacy Commissioner – to bring privacy law into the digital era including in particular enhanced enforcement powers to address the wider scope of collection and uses of data through technology and digital means. As was demonstrated in the 2018 Facebook/Cambridge Analytica debacle, there are far-reaching implications for the potential for unauthorized uses of personal data through digital media and in particular through social media.

There have been strong urgings to adopt a law similar to the EU's *General Data Protection Regulation* ("GDPR") – which includes a rights-based approach to privacy, prescriptive rules for uses and accountability, and most significantly, very significant potential financial penalties for non-compliance. However a contrary view expressed in many Canadian sectors – particularly business stakeholders – is that the principles-based approach of PIPEDA should be maintained, with appropriate increased enforcement powers.

The CPPA arguably seeks to steer a middle course – adopting a number of enhanced prescriptive rules reflective of the GDPR's more stringent regime but at the same time preserving the Canadian privacy experience under PIPEDA – informed by that statute's more flexible principles-based approach.

In many respects, the CPPA achieves what might be characterized as "a fine balance" between adopting a GDPR-like statute and preserving PIPEDA's frame of reference. Most significantly, the CPPA retains – now within the statutory text as opposed to in a schedule – PIPEDA's ten *Fair Information Principles.* However it builds into this framework significant express GDPR rights, or versions of them, including the right to be forgotten, the right to portability, and the right to be informed of the implications of automated processing.

Regulatory enforcement regime

Significantly, the CPPA adopts an enforcement regime that is very GDPR-like – providing for the most severe potential financial penalties under any current privacy regime married to an order-making power for the OPC. The financial penalty regime is qualified in a very Canadian way. Depending on the nature and severity of the non-compliance, penalties are imposed by the new Personal Information and Data Protection Tribunal or fines are sought through prosecutions brought in court.

This penalty framework is analogous to Canada's competition law enforcement regime whereby the Commissioner of Competition undertakes investigations and, where warranted, seeks administrative monetary penalties before the Competition Tribunal, or alternatively recommends prosecution for offences, punishable by fine or imprisonment. If the recent competition enforcement experience can offer guidance, few applications to the Tribunal will be litigated, or prosecutions brought. Instead, consent settlement agreements between the Privacy Commissioner and non-compliant parties are likely to be the norm, providing for both compliance obligations and monetary penalties.

Private right of action

The CPPA introduces a statutory private right of action, accessible to anyone impacted by a breach under the Act. This right expands the scope for available remedial actions from that currently provided in PIPEDA – where only a person who has made a complaint to the OPC can commence an action. The new right will enable a much wider scope for class actions. However its availability is conditioned on the Commissioner or the Tribunal making a finding of breach or a prosecution resulting in a conviction.[1] The scope for class actions will be significant since to recover damages an injured party must show actual harm or injury, which on an individual basis likely would not warrant making a claim.

Individual's control of their information – consent retained, enhanced

Significantly, the CPPA retains consent as the key control right for individuals with respect to their personal information. By contrast, the GDPR stipulates that personal information must be processed lawfully, providing consent as only one of several bases for lawful processing. The CPPA in some respects seeks to enhance an individual's control over their personal information. A more prescriptive definition of "consent" harkening to the OPC's 2018 *Guidelines for obtaining meaningful consent* is stipulated. Enhanced transparency rights – for example requiring plain language privacy policies and procedures and the right to request an explanation for automated decision-making, as well as the new rights of deletion and portability – support this heightened emphasis on an individual's control over their personal information.

Transparency

Related to the emphasis on enhancing individual control are the Act's provisions requiring organizations to be transparent in providing information regarding the practices, procedures and policies relating to their collection and use of personal information. These include requiring that publicly available policies and procedures, disclosures in connection with obtaining consent, information provided in response access requests, and explanations regarding automated processing – are to be provided in plain language.

[1] By contrast the PIPEDA right does not require any finding of breach by the Commissioner; PIPEDA ss.14-16.

Accountability – privacy management programs

The CPPA strengthens PIPEDA's Accountability Principle by expressly requiring organizations to have a privacy management program incorporating its policies, procedures and practices for compliance with the Act and to have such documents available for the Commissioner to examine on request. While not following the chapter and verse of the Commissioner's guidance document, "Getting Accountability Right with a Privacy Management Program",[2] it can be understood that the thrust of this new provision is compliance in accordance with that document. Consistent with the OPC guidance, the CPPA stipulates that a privacy management program should take into account the volume and sensitivity of the personal information held by the organization.

Exceptions to consent

Seeking to address circumstances where express consent may be either difficult to obtain or not appropriate, the CPPA includes expanded exceptions to the consent requirement, including for designated "business activities", "socially beneficial activities" and de-identified information. While these exceptions arguably derogate from the goal of enhancing the control that an individual has over their information, they are seen as facilitating the dynamics of collection and use of personal information in circumstances where consent would be understood and therefore unnecessary to address, as well as encouraging innovation through the use of personal data, appropriately de-identified. To be noted, there is no express right for an individual to object to such collection or uses.

Potentially the most expansive and privacy-limiting exception is the new category of "business activities", listed, not exhaustively, to include uses related to providing a product requested by an individual, or necessary for an organization's security, or for product safety purposes, and – significantly – activities where an organization does not have a direct relationship with an individual and where obtaining their consent would be impractical. This last category – which may be intended to include circumstances of data analysis for third party assessment requirements such as insurance – has the greatest potential impact within the digital environment including online tracking, social media platforms and search engines.

However two important conditions are stipulated for any such non-consented business activity collection or use. Firstly, such collection or use must be expected by a reasonable person, and secondly, the information must not be collected for the purpose of influencing an individual's behaviour or decision. This second condition likely eliminates much of the potential for non-consented Internet tracking for purposes such as targeted advertising.[3]

[2] Published jointly with the Offices of the Information and Privacy Commissioners of Alberta and B.C.
[3] The consent exception category of third party business activities harkens to the GDPR's "legitimate interests" category which requires that the collection or use must be within the reasonable contemplation of the affected individual, meaning in effect implied consent. However the added limitation that purposes may not include influencing an individual's behavior or decisions suggests a more restrictive approach than under the GDPR.

Notwithstanding the limiting aspect of this second condition, the scope for non-consented collection or use of personal information through indirect means in connection with an organization's business activities appears potentially to be very wide.

What is not included

The CPPA arguably falls short of a number of objectives set out by commentators as reasonable expectations for this opportunity to bring Canada's privacy laws into the modern era.

Most glaring is the omission of expressly extending the law to political parties and their related actors, urged by both diverse commentators as well as by the parliamentary Committee on Access to Information, Privacy and Ethics (the "ETHI Committee"). Related to this missed opportunity to clearly extend our privacy laws to the elections ecosystem appears to be a narrowing of the application of the new law with respect to charities and other not-for-profit organizations which have compliance obligations under PIPEDA with respect to their commercial activities but under the CPPA potentially may not be subject to any compliance requirements.[4]

Another area in which the CPPA falls short of expectations is the treatment of rights with respect to automated processing of data (read algorithmic modeling). The CPPA adopts the GDPR's impactful requirements relating to transparency for individuals affected by automated processing methodologies (such as for example online tracking and targeting) by requiring disclosure of such methodologies and providing an individual the right to receive an explanation of any prediction, recommendation or decision made by such automated processing system about them. However the CPPA does not contain the correlative express right to object to an organization's using such automated processing/decision-making, as is provided in the GDPR.[5] Under the CPPA, any such right would need to be exercised through the right to withdraw consent or the right to be forgotten – which would be at best an indirect and more complicated avenue to achieve such this result.

Significantly, merely days before the tabling of Bill C-11, the federal Privacy Commissioner released his report and recommendations for regulatory reform coming out of his in-depth consultation into the privacy implications of artificial intelligence (AI).[6] The Commissioner's recommendations set forth two explicit rights of individuals with respect to automated processing – the right to a meaningful explanation of automated

---

[4] Under PIPEDA "commercial activity" is defined to mean essentially a "transaction, act or conduct or any regular course of conduct that is of a commercial character", which would include commercial activities of charities, such as fund-raising events. Under the CPPA commercial activity is proposed to be defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, taking into account an organization's objectives for carrying out the transaction, act or conduct, the context in which it takes place, the persons involved and its outcome", suggesting that if a particular transaction even if narrowly commercial has a non-commercial objective such as carrying out an organization's non-commercial activities, it may not be considered commercial for purposes of the CPPA.

[5] Quebec's recently tabled proposed legislation to update its privacy law, Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, while not providing for an express right to object permits affected individuals to submit observations and require a re-assessment of any decision made by such system.

[6] *A Regulatory Framework for AI: Recommendations for PIPEDA Reform*, Office of the Privacy Commissioner, November 2020

processing affecting them, and the right to contest automated decisions including those where consent has been given and those where an exception to consent was relied on.

Promoting innovation

An important dictate in the government's bringing forth the new privacy law is to encourage innovation. Understandably, achieving this result at the same time as enhancing individuals' control over their personal information points to a potential conundrum: innovation (read big data/algorithmic models/automated processing) requires access to huge databases of personal information. The CPPA seeks to respond to this dictate through the new circumstances for exceptions to consent, noted above, together with provisions enabling de-identified information to be used for research and related purposes without consent. Also supporting this innovation thrust of the CPPA is the proposal for statutory recognition of codes of practice, meeting criteria set out in the regulations, that may be certified by the OPC and which could enable innovation strategies of organizations seeking to adopt AI systems leveraging the collection and use of de-identified information.

Conclusions

The proposed CPPA provisions for Canada's new national privacy law contain many detailed stipulations that will have diverse impacts for businesses and private individuals alike. A nuanced analysis of these provisions will require close scrutiny not only to understand their potential impact and compliance requirements but also to identify considerations for potential adjustments prior to enactment of the legislation.

Bill C-11 will be reviewed by a parliamentary committee (either the Committee on Industry, Science and Technology or the ETHI Committee). It can be expected that there will be a significant number of submissions to the Committee addressing both perceived omissions in the legislative regime as well as concerns regarding the impact and in some instances the lack of clarity of certain of its provisions.

The government has indicated an 18-month transition period for the legislation to take effect following enactment. Sensibly, given the breadth and potential impact of the new law, one can expect at least a six-month period for review and debate before the Bill is adopted into law, implying a timeline of not earlier than January 2023 for the Act to come into force.

For more information please contact:
David Young 416-968-6286 david@davidyounglaw.ca
Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.