November 30, 2020

Canada's Proposed New Consumer Privacy Protection Act: The Good, the Bad, the Missed Opportunities

By: Emily Laidlaw

Bill Commented On: Bill C-11, *Digital Charter Implementation Act, 2020*, 2nd Sess, 43rd Parl, 2020 (first reading 17 November 2020)

On November 17, 2020, the Federal Government unveiled the most sweeping consumer privacy law reform in the last twenty years with the proposed *Digital Charter Implementation Act, 2020* (Bill C-11). The Act would repeal and replace parts of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (PIPEDA) with a new private sector privacy statute, the *Consumer Privacy Protection Act* (CPPA) (not to be confused with the well-known *California Consumer Protection Act* (CCPA)), and would enact the *Personal Information and Data Protection Tribunal Act* (Tribunal Act). The Bill makes good strides in modernizing Canada's privacy legislation. It is also, in the end, a missed opportunity for more profound law reform.

If passed, it will necessitate modernization of Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5 (PIPA). PIPA is designated substantially similar legislation, meaning that PIPA rather than PIPEDA regulates personal information within our provincial borders (and through our ombudsman, the Office of the Information and Privacy Commissioner of Alberta). Without this designation, PIPEDA would apply to all consumer privacy transactions within Alberta. As will be detailed below, Bill C-11 fundamental revamps consumer privacy legislation and therefore unless Alberta follows suit, it is highly unlikely the substantially similar designation can be maintained.

Bill C-11 has been a long time coming. The Federal Government has identified privacy reform as a priority (e.g. here, here and here). It is a central feature of Canada's Digital Charter, which communicates the Federal Government's mandate and priorities for law and policy reform concerning the digital economy set down through Innovation, Science and Economic Development Canada. The Digital Charter identifies PIPEDA reform as a priority, including specific proposals in the Government's white paper *Strengthening Privacy for the Digital Age*. The white paper takes into account several recent recommendations for reform put forth by the Standing Committee on Access to Information, Privacy and Ethics (e.g. here and here). The Federal Privacy Commissioner, Daniel Therrien, has also made bold recommendations for reform in recent annual reports (here).

Domestic law reform is taking place against a world stage where private sector privacy– or more specifically data protection – law reform is evolving swiftly with significant impact on global commerce and trade law (e.g. see the digital trade provisions of the United States Mexico Canada Agreement). Notable are Europe's General Data Protection Regulation, 2016/679 (GDPR) and California's CCPA, mentioned above. The GDPR, in particular, imposes stringent

privacy and data protection rules on the private sector with extra-territorial reach. If Canada does not amend PIPEDA, there is a risk that the law will not be deemed equivalent to maintain cross border data flows with Europe. At the same time, domestic legislation like the *Illinois Biometric Information Privacy Act*, 740 Ill. Comp. Sta. 14, and to a lesser extent the CCPA, introduce a technology angle to privacy legislation, focused on pressing current challenges in areas of biometric data and the data brokerage industry. All this to say that consumer privacy laws are all the rage right now, and PIPEDA was long overdue for reform.

As explained, Bill C-11 would enact the CPPA and Tribunal Act. The CPPA converts PIPEDA's principles-based approach in its Fair Information Principles (PIPEDA, Schedule 1) to substantive rules. The Fair Information Principles have been the subject of significant criticism, and the move to embed concepts like security safeguards, consent and accountability as operable rules is a welcome and practical shift.

The most significant overhaul is as to the Office of the Privacy Commissioner (OPC) oversight and enforcement. The Bill would change the OPC from an ombudsman model to a regulator more akin to European data protection authorities. At the moment, the OPC is rather toothless, and its chief power is to name and shame organizations that failed to comply with its recommendations. This was most recently exposed in the joint investigation of Facebook by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia in the wake of the Cambridge Analytica scandal. Facebook not only refused to comply with their recommendations, but the investigation revealed that Facebook failed to implement commitments it made to the OPC following a 2009 investigation. Pursuant to the CPPA, the Privacy Commissioner would have order making power (ss 92, 103) and organizations that breach the Act would face the risk of fines of up to 5% of gross global revenue or $25 million (a higher maximum fine than the GDPR's 4% of global revenue) (ss 94(4), 125).

The Tribunal Act would establish a Personal Information and Data Protection Tribunal (s 4), a significant step in formalizing adjudication of privacy infringements and an appeals process. The tribunal would hear appeals from "findings, orders or decisions" of the Privacy Commissioner (CPPA, s 100). The Tribunal's remit is also to assess and impose fines. Indeed, the Privacy Commissioner can only make recommendations as to a fine, and the power to impose the fine rests with the Tribunal (CPPA, ss 93-94). As Michael Geist has commented, the rationale for the composition of the Tribunal is unclear. The Tribunal would be comprised of three to six members, and only one member needs to have expertise in information and privacy law (Tribunal Act, s 6). This is odd as the benefit of tribunal models tends to be their subject matter expertise, and in this complicated and evolving area subject matter expertise seems all the more important.

The most profound missed opportunity in Bill C-11 is the failure to incorporate recommendations of the Privacy Commissioner that PIPEDA should be reformulated as a rights-based framework. Daniel Therrien commented:

> Privacy is much broader than data protection – although data protection seeks to participate in the protection of privacy. Neither of the two federal statutes formally

> recognizes privacy as a right in and of itself. If these laws are to meaningfully protect the broader right to privacy, this objective needs to be reflected more explicitly.

It is unclear why Bill C-11 is drafted this way. The GDPR, which influence on this Bill is clear, is rooted in a rights-context. Data protection and privacy are independent fundamental rights in the *Charter of Fundamental Rights of the European Union*, 2012/C 326/02. That they form the interpretive context of the GDPR is evident in recent Court of Justice of the European Union judgments in *Schrems I and II*. Littered throughout Bill C-11 are human rights principles of minimal impairment, necessity and proportionality, in particular in the CPPA. Teresa Scassa identified these principles as operating in sections 12 and 13 of the CPPA regulating appropriate purposes and limitations for personal information collection, use or disclosure (recording of panel discussion available soon), but similarly laments the lack of commitment to a rights-based framework more generally. Rights language is observable elsewhere in the CPPA, with requirements to examine the privacy implications of cross border data flows (s 62) and use proportionality as the metric in assessing de-identification of personal information (s 74). The way the CPPA is written, it imports a rights narrative without rooting it in a rights framework that would shape its interpretation. This separates the CPPA from the body of law and policy in privacy that should inform its meaning. Privacy is a human right recognized in Article 12 of the *Universal Declaration of Human Rights* and Article 17 of the *International Covenant on Civil and Political Rights*, a protected *Charter* right (sections 7 and 8), and the subject of significant scholarly and policy attention. Consumer privacy legislation that does not acknowledge the right to privacy is a glaring absence. It misses the elephant in the room in terms of the privacy threats we face, and fails to provide direction to the Privacy Commissioner, new Tribunal and courts that will be tasked with interpreting the provisions.

In many respects the Bill proposes meaningful amendments to data protection law that would strengthen consumer privacy and bring our laws more closely in line with the GDPR. Some of the significant changes proposed in Bill C-11 are as follows.

Consent

The CPPA seeks to modernize the consent rules, simplifying consent in two ways: (1) imposing plain language requirements to enable meaningful consent, which is mentioned in various places; and (2) simplifying the circumstances where consent is not needed. For example, the CPPA carves out an exception from the requirement of express consent where "the organization establishes that it is appropriate to rely on an individual's implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed" (s 15(4)). This is a potentially expansive exception, and without a rights-based framework, there is nothing to constrain it in a meaningful way. A concerning provision is section 18(2)(e), which provides that a business does not require consent to collect or use (note disclosure is not included) data where it would be impractical because there is no direct relationship between the organization and the individual. This would exclude some of the more pernicious aspects of consumer data brokerage, which is indirect between the organization and the individual.

In some ways it is disappointing that consent continues to be the driving force of the CPPA, although it would be impractical to move away from a consent framework entirely, in part to be interoperable with the GDPR, CPPA and similar legislation. Bill C-11 attempts to strike a middle ground. As the Fact Sheet explains, the federal government aimed to remove "the burden of having to obtain consent when that consent does not provide any meaningful privacy protection." From a social media security perspective, this is a space where data flows are complex. They are shared spaces that exist so that individuals publicly disclose personal information. The data generally cross borders in real time and in multiple directions. Some of the big risks are inferential data, the seemingly mundane data that are compiled to create profiles about an individual. For example, sensitive data about political views, health or sexuality can be generated by algorithms using ordinary data and behavioural insights, which can then be used to make decisions that impact an individual, such as differential pricing. And the data is often collected in social media spaces that are designed and curated to keep user attention and interaction. This increasingly ordinary narrative our experiences in the digital economy is only indirectly served by the CPPA. However, it is notable that the GDPR fails to adequately address inferential data as well.

User Empowerment

The CPPA introduces a suite of amendments that are similar to provisions introduced in the GDPR strengthening user empowerment to control their online identities. They include:

- *The right of data portability*: This allows an individual to transfer their personal information from one organization to another (s 72). This is more limited than in the GDPR, at least for the time being, to companies in the same sector or industry (see here) More generally, the right does not address broader issues of interoperability between different ecosystems online, although this is also a criticism of the GDPR.
- *The right to withdraw consent*: This existed under PIPEDA's Fair Information Principle 4.3.8, but it is a broader right in the CPPA because it can now only be limited via *reasonable* terms of contract (s 17).
- *The right to require personal information be deleted*: This is a new right with a similar objective as the right of erasure in the GDPR. Under PIPEDA, consumers have rights of access and to challenge the accuracy of personal information, but consumers do not have the power to demand deletion of personal information. The CPPA introduces such a right, but it is limited to information the organization collects from the individual, thus excludes inferential data (s 55(1)). However, the CPPA extends the right of deletion to third party service providers, requiring that the organization inform the service provider of the deletion request and obtain confirmation the personal information was disposed of (s 55(3)). Service providers is a defined term and would include activities related to supply chains and cloud providers. It means that consumers would have a right of deletion for the data an organization transfers to "a parent corporation, subsidiary, affiliate, contractor or subcontractor, that provides services for or on behalf of another organization to assist the organization in fulfilling its purposes" (s 2).
- *Private right of action:* The CPPA creates a limited private right of action for damages. An individual is enabled to start an action, but only after an adverse finding of the Privacy Commissioner or Tribunal, or where an organization is convicted of an offence (s 106).

- *De-Identification:* The CPPA clarifies the rules for use of de-identified data (data that has been stripped of personally identifiable markers) and seeks to balance enabling use of such data against protection of personal information. De-identified data may be used for internal research and development (s 20). The CPPA introduces the idea of a "socially beneficial purpose", which is the basis for which de-identified data may be shared by private entities with public entities, such as for health, infrastructure or the environment (s 39). The CPPA prohibits identifying individuals using de-identified data (s 75) and mandates security safeguards relative to the sensitivity of the data (s 74). The de-identification provisions were strongly criticized by the Public Interest Advocacy centre as weakening previously held privacy rights by removing the consent requirement (see discussion here).
- Notably absent from the CPPA is making explicit a broad right to be forgotten. An interpretation of PIPEDA that gives effect to a right to be forgotten was proposed by the Privacy Commissioner in 2018 and a reference is pending before the Federal Court (I examined the initial proposal here).

Automated Decision Making

The CPPA introduces a broad right to explanation concerning automated decision systems. Automated systems are not defined in the Bill. Consumers would be entitled to an explanation of a "prediction, recommendation or decision" using an automated decision system (s 63(3)). This is a broader right than in the GDPR, which narrowly applies to wholly automated decisions which have a significant impact on an individual (Article 22(1) and (2)). The CPPA, rather, seems to target any use of automation systems such as artificial intelligence or algorithms, and broadly grants the right for any prediction, recommendation or decisions. However, section 63(3) does not address the other side of the coin, where the organization does not make use of an automated decision system, but rather is the source of the data that other entities use for their automated decision system (consider data brokers). In contrast, the CCPA is more direct in addressing these kinds of issues. For example, consumers can opt out of the sale of data to third parties and these third parties need to notify consumers if they want to sell their data and give them the opportunity to opt out (§1798.120 and §1798.115(d)).

Codes of Practice

One of the most interesting provisions in the CPPA is encouragement of the use of codes of practice. Entities (which is broader than the organizations to which the Act would apply), would be able to ask the Privacy Commissioner to review and approve their codes of practice and certification schemes (s 76). Since all organizations to which Act would apply would be required to create a privacy management programme (s 9), this next step is a way for organizations to both create something bespoke to their organizational needs and receive the OPC stamp of approval.

Cross Border Data Flows

Section 62 provides that to fulfil openness and transparency obligations, organizations must disclose if they carry out cross border data transfers or disclosures "that may have reasonably

foreseeable privacy implications". This provision was noted above as an example of rights language begging for a rights framework. However, the provision is notable for another reason. It complements legal developments in Europe, in particular *Schrems II*. One of the issues in *Schrems II* was the validity of standard contractual clauses (SCCs), which have developed as a way for data exporters to satisfy the criteria of appropriate safeguards in situations where there is no adequacy or equivalence agreements between states. *Schrems II* concerned the sufficiency of privacy protections of data transferred to the United Stated because of the surveillance programmes made famous by Edward Snowden. The CJEU, among other things, validated the use of SCCs, but held that organizations must assess the adequacy of privacy protections of the third-party countries. In November 2020, the European Data Protection Board issued two recommendations (here and here) detailing a framework to analyze the sufficiency of foreign surveillance laws. The CPPA uses simpler language and is indirect in its approach, but the consequence is similar. If an organization must make available in plain language "whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications" (s 62(2)(d)), it must first assess the privacy implications of any of its cross border data transfers.

While the privacy risks of cross border data transfers necessitate greater organizational responsibility, an obligation like this will face serious challenge from industry, because it is resource-intensive even for the most sophisticated company. Indeed, one criticism of Bill C-11 is that greater strides could have been made to address the scalability of the obligations and needs of small and medium sized enterprises (SMEs). The CPPA provides that the Privacy Commissioner, in the exercise of its duties, "must take into account the size and revenue of organizations, the volume and sensitivity of the personal information under their control and matters of general public interest" (s 108). It is understandable that SMEs were not addressed directly. It is not an issue that can be easily resolved, where even the smallest company can have significant global impact (consider the size of Cambridge Analytica compared to the impact of its data practices). Nevertheless, companies will face considerable hurdles in operationalizing this obligation, among others.

It is unclear at this stage what the final shape and content of Bill C-11 will be. At the time of writing, it has only been introduced and received the First Reading in the House of Commons. I expect it will pass in some form – the pressure for equivalence with the GDPR and to keep pace with the CCPA is strong. And then it will be Alberta's turn to modernize PIPA to be substantially similar.

This post may be cited as: Emily Laidlaw, "Canada's Proposed New Consumer Privacy Protection Act: The Good, the Bad, the Missed Opportunities " (November 30, 2020), online: ABlawg, http://ablawg.ca/wp-content/uploads/2020/11/Blog_EL_Bill_C-11_CPPA.pdf