David Young Law
Compliance Bulletin

June 2021

Does the Privacy Commissioner's ETHI Submission mean a Bill C-11 rewrite?

In its May 11, 2021 Submission to the Parliamentary ETHI Committee,[1] the Office of the Privacy Commissioner (OPC) delivered a severe critique of Bill C-11, the government's proposed global revision to the current federal privacy law, PIPEDA,[2] arguing that in its present form the Bill would represent a step back overall for privacy protection in Canada. Almost coincidentally, on June 4, the Prime Minister announced the re-appointment of the current Commissioner, Daniel Therrien, for a one-year term. These two events, although not related, present an interesting backdrop to the future course of privacy reform at the federal level in Canada.

Why does the OPC say that the Bill as drafted would represent a step back? In general terms, because in its view the Bill, although seeking to address most of the privacy issues relevant in a modern digital economy, does so in ways that are misaligned and less protective than laws of other jurisdictions. More specifically, in the OPC's view: because the provisions meant to give individuals more control give them less; because the increased flexibility for organizations to use personal information without consent do not come with additional accountability; because administrative penalties will not apply to many of the most frequent and important violations, in particular those relevant to consent and exceptions to consent; and because the OPC would not have the tools required to manage its workload to prioritize activities that are most effective.

The OPC submits that this potential impact can be reversed and the new law can become a strong protection for the privacy rights of Canadians if some important amendments are made, under three key themes:

- a better articulation of the weight of privacy rights versus commercial interests;
- enhancing specific rights and obligations; and
- the role of the OPC and access to quick and effective remedies.

Privacy as a fundamental human right

Probably the OPC's most overarching criticism is the Bill's failure to enshrine the primacy of privacy interests relative to commercial interests – instead in effect providing that they must be balanced against one another. In fact, the OPC sees the Bill as enabling greater flexibility for organizations to collect and process personal information for commercial purposes without sufficient weight given to protecting privacy. To address this perceived imbalance of protection, the OPC recommends the inclusion of a Preamble chronicling the quasi-constitutional recognition of privacy as a human right with sufficient weight to ensure that the added commercial flexibilities provided in the Bill are exercised in a context of first and foremost protecting privacy.

---

[1] Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the *Digital Charter Implementation Act, 2020,* May, 2021 to the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[2] *Digital Charter Implementation Act, 2020* repealing the *Personal Information Protection and Electronic Documents Act* and enacting the *Consumer Privacy Protection Act.*

In his prefatory comments to the Submission, the Commissioner states this objective as follows:

> In my view, it would be normal and fair for commercial activities to be permitted within a rights framework, rather than placing rights and commercial interests on the same footing. Generally, it is possible to concurrently achieve both commercial objectives and privacy protection. However, when there is a conflict, I believe rights should prevail.

In addition to the proposed Preamble, the OPC recommends a strengthened "Purpose" clause that would recognize privacy as a quasi-constitutional right as opposed to characterizing them in a narrow and technical sense (in the OPC's view), provide a greater weighting for privacy rights by adding privacy considerations to balance new, evolving economic idioms and provide a more clear statement of the law's purpose and constitutional grounding. Specifically, the OPC would see the key precepts of proportionality, transparency and accountability written into the purpose clause, as opposed to stipulating them simply as requirements for specific rules, as well as adding the GDPR precept of fairness, not currently reflected in Bill C-11. In addition, the purpose clause would clearly state the right of privacy of individuals to be a fundamental right.

The OPC contexts in part this enhanced status for privacy within its recognition that in the modern digital economy a strict adherence to a consent regime for collecting and using personal information is unrealistic and that alternative mechanisms need to be adopted. To balance this greater flexibility, the OPC sees the recognition of the fundamental human right status of privacy as a bulwark for privacy protection in instances where prescriptive consent mechanisms are not appropriate.

In addition, the OPC recommends specific wording changes to sections 12 and 13 of the Bill (Appropriate Purposes; Limiting Collection) to more explicitly address the appropriateness and specific reasons/purposes (specific, explicit and legitimate) for collecting and using personal information, in the context of the fundamental right.

Consent model

The OPC criticizes Bill C-11's proposed adjustments to the existing wording found in PIPEDA arguing that they would lessen the threshold for ensuring "valid" consent - specifically, the requirement that an individual "understand nature, purpose, and consequence of [the activity to which they are consenting]", replacing this requirement with a prescription simply to address certain minimum elements, in plain language, in an organization's privacy policies.[3]

In the OPC's view, by prescribing elements of information to appear in privacy notices without maintaining the requirement that consumers must understand what they are asked to consent to, Bill C-11 does not achieve its goal of giving individuals more control over their personal information, but instead provides less control. This result is exacerbated by the open-ended nature of the purposes for which organizations may seek consent.

The OPC states that the Bill places too much emphasis on providing organizations flexibility in defining the purposes for which personal information may be used and in obtaining consumer consent. In its view, objective standards such as in section 6.1 of PIPEDA (the "understanding" factor) and the requirement that purposes be defined in a specific, explicit and legitimate manner, as set out in Principle 4.3.3 of PIPEDA, are required to achieve the proper level of protection.

[3] Along similar lines as are set out in the OPC's *Guidelines for obtaining meaningful consent* (May 2018)

Exceptions to consent

In terms of added flexibility to use personal information without consent, the OPC agrees that in today's more complex digital economy such flexibility is important because in many contexts meaningful consent may not be appropriate or even achievable. However the OPC criticizes Bill C-11's approach to an expanded listing of exceptions to consent in two important respects. Firstly, in its view, some of the added exceptions are unreasonably broad, or undefined. Secondly, the Bill does not impose a more rigorous accountability regime to ensure that organizations' expanded uses of personal information without consent meet the OPC's recommendations for the law's minimum standards for privacy protection (read – fundamental human right, more prescriptive purpose clause).

The OPC echoes criticism from other sources that the "commercial risk" exception, without an appropriately narrow definition, is open to abuse – such as to include almost any activity of an organization. Secondly, the OPC takes square aim at the open-ended potential scope of the s. 18(2)(e) exception regarding activities for which obtaining consent would be impracticable because the organization does not have a direct relationship with the individual. In the OPC's view, the potential scope of activities which could fall under this exception is extremely broad, querying whether there are any real limitations on the kinds of activities which could be included. The overarching requirement - that "a reasonable person would expect such a collection or use" as prescribed by s. 18(1)(a) - in the OPC's view, fails to provide consumers with any certainty as to how their personal information will be used, moreover, by an organization they likely do not know.

The OPC notes that it should be obvious to individuals why any of the various provisions of s. 18(2) (business activities for which consent is not required) could permit such an activity without consent. For instance, paragraphs 18(2)(c) and (d) address enabling network security and product safety, respectively. Other exceptions to consent point to specific purposes and activities such as preventing or investigating financial abuse or fraud.

However, this is not the case with respect to proposed paragraph 18(2)(e). In the OPC's view this paragraph removes the consent requirement from certain activities simply because obtaining consent is impracticable, not because there is an offsetting benefit to justify such an action. In other words, in the OPC's view, the fundamental principle of consent is put aside for the simple reason that it is impractical to obtain it.

As an alternative to the current approach to unconsented uses reflected in s. 18(2), the OPC proposes an exception to consent based on "legitimate commercial interests". In its view, such an exception would provide flexibility to authorize unforeseen reasonable purposes but, unlike paragraph 18(2)(e), would be based on the particular and knowable purposes being pursued by the organization.

On the other hand, the OPC states that such an exception should only be permitted in a rights-based regime, as it proposes. Other preconditions for such an exception should include the completion of a privacy impact assessment (PIA) and a balancing test similar to that found under the GDPR's legitimate interests rule.

Finally, while in principle agreeing with the concept of permitting de-identified information to be used without consent for socially beneficial activities, the OPC states that as currently written, the exception is completely open-ended and should be supplemented by prescriptive requirements relating to approval of applications for such uses, prohibitions against using the information for other purposes, or re-identifying it, and providing a definition of what is socially beneficial to ensure that it cannot mean simply private or commercial interests.

Accountability regime

The OPC argues that the increased flexibility afforded by Bill C-11 – particularly where exceptions to consent are introduced – needs to be accompanied by increased corporate responsibility.

In the OPC's view, accountability is one of the primary counter-balances to the increased ability for organizations to use information without consent. As such, it is critical that the accountability principle be clearly defined and protective measures stipulated such that the accountability of organizations is real and demonstrable.

In the OPC's view, Bill C-11 does not define accountability, except indirectly and implicitly through the requirement in s. 9 to document, under the concept of a "privacy management program," certain policies, practices and procedures: section 9 does not set an objective standard for what is accountability; it is merely descriptive.

The OPC states that the elements of an organization's privacy management program should meet the objective standard of providing accountability designed to achieve compliance with the law including, as stipulated elements, policies, practices and procedures designed to ensure such compliance.

Furthermore, the OPC argues that accountability should be demonstrable, through a requirement for organizations to maintain sufficiently adequate records of its processing activities to establish compliance with the law, to design all programs involving processing of personal information on the basis of privacy by design, and for activities involving high-risk, to conduct PIAs.

Specific rights of individuals – ADS, erasure, mobility

The OPC argues for enhancement of three new rights provided in Bill C-11 – the right to explanation of automated decision-making (ADS), the right of erasure, and the right to data mobility.

With respect the latter two rights, the OPC argues that they should extend to *all personal information* of an individual held by an organization, not just personal information collected directly from an individual, which in many cases would represent only a small portion of the information it holds about the individual. So the right of erasure (right to be forgotten) would extend to search engine indexes and information held by data brokers. The right to mobility would include information derived or inferred from the individual's personal information including, for example, risk assessments conducted by financial institutions.

With respect to rights relating to automated decisions, the OPC believes that modifications are necessary to denote a clearer standard for explanations of such decisions affecting an individual, to create a right to contest automated decisions, and to strengthen accountability through privacy by design and algorithmic traceability.

Regarding the *right to explainability*, the OPC states that the current obligation under Bill C-11 does not provide consumers with the ability to obtain a meaningful explanation. It provides the right to know the prediction or decision, and the provenance of the information upon which this was based, but not the relationship between the personal information and the decision, nor the elements of personal information relevant to the decision. The OPC recommends that the standard for explanation be enhanced to allow individuals to understand: (i) the nature of the decision and the relevant personal information relied upon, and (ii) the rules that define the processing and the decision's principal characteristics.

Additionally, individuals should be provided with a *right to contest* automated decisions. Such a right would be consistent with the approach taken in other jurisdictions, including Europe under the GDPR and Quebec under

Bill 64. The right to contest would be in addition to the ability to withdraw consent currently provided for in Bill C-11. The OPC's view is that both rights are necessary, as withdrawal of consent is an all-or-nothing decision, whereas contestation provides individuals with recourse even when they choose to continue to participate in the activity for which ADS was employed.

Cross-border data flows

The OPC recommends that a separate section be added to Bill C-11 containing specific provisions applicable to trans-border data flows, so as to enhance transparency and accountability. Four key considerations should be addressed, specifically:

- To whom should the rules apply? – expand beyond conventional service provider processing to other relationships in the digital environment;
- Who is accountable – the transferring organization or the offshore service provider, or both?
- Preconditions for any transborder transfer of data such as equivalency regarding the level of protection provided by the offshore service provider; and
- Assessing the level of protection under the privacy regime in the destination jurisdiction.

The OPC in an Annex to its Submission sets forth fourteen separate recommendations for a comprehensive regime to regulate transborder data flows, including: more explicit disclosure in organizations' policies and procedures of the nature of their transfers and the risks involved; standardized requirements for service provider contracts; obligations on transferring organizations to conduct assessments of equivalent protection and the authority of the OPC to review such assessments and prohibit transfers where sufficient protections are not in place; and the extension of the transborder rules to *disclosures* between organizations in addition to their application to "transfers".

While the proposed transborder regime would significantly enhance the hands-on application of the law to such transactions, it does not go as far as the GDPR adequacy rule or the somewhat analogous Bill 64 requirement for approved jurisdictions to avoid that proposed law's requirement for a PIA as a condition for transfers to non-Quebec jurisdictions.

Enforcement and oversight provisions

The OPC makes a series of recommendations addressing what it views as would be improvements in the effectiveness and access to remedies under Bill C-11. These include expanding the substantive provisions of the law for which non-compliance can result in administrative penalties, eliminating the proposed Personal Information and Data Protection Tribunal thus giving the OPC the power to impose AMPs directly, enhancing the investigate powers of the OPC including the right to conduct pro-active audits, giving it greater discretion in conducting investigations and resolving complaints, and in cases of breaches resulting from deficient security safeguards, the power to order compensation for damages suffered by individuals .

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca