David Young Law
Compliance Bulletin

March 2022

Privacy law reform – will it be harmonized?

One of the hot topics of debate among privacy law experts is whether the current reform initiatives will, or should, result in harmonization across federal and international jurisdictions. Or, put differently, should federal, provincial and international privacy law regimes be "interoperable"? [1]

Efficiency as the objective

As the BC Information and Privacy Commissioner put it eloquently at the recent Vancouver conference, a commonality is needed to address today's reality of ubiquitous data flows across borders. The privacy ecosystem needs mechanisms to get along – both internationally and nationally.[2]

Within this frame, it can be posited that the main objective of harmonization is *efficiency* – resulting from achieving commonality among privacy law regimes. What does this mean for stakeholders?

Efficiency for the actors governed by the laws – the data collectors – means efficiencies of compliance procedures developed to meet the statutory requirements.

Efficiency for the individuals – or "data subjects", for whose benefit the laws exist - means efficiencies in understanding the protections provided and in being able to realize them.

Efficiency for the regulators exercising oversight - means being able to apply and enforce the laws in a manner that is fair, and encourages compliance by organizations across all jurisdictions. It also means enabling regulators to communicate to the public a seamless, consistent framework for privacy protection across those jurisdictions.

Current legal landscape

The EU's *General Data Protection Regulation* (GDPR) set a new standard for privacy law rigour when it came into force in May 2018 – not only in substantive compliance requirements but also in the magnitude of financial penalties for non-compliance. Reform initiatives in both Canada and the US have drawn inspiration from it – reflecting what may fairly be characterized as the era of second-generation privacy laws, encompassing enhanced protections for the digital era, married to mechanisms for facilitating for innovation.

[1] This Bulletin reflects my notes for the panel discussion, "Canadian Private Sector Privacy Law Reform: Federal and Provincial Initiatives and Their Interoperability" at the 2nd Annual Vancouver International Privacy & Security Summit, March 9 -11, 2022.

[2] Keynote Address, "Law reform in the time of COVID-19" at the VIPSS.

David Young Law • Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
Privacy and Regulatory Law Counsel • davidyounglaw.ca

At the Canadian federal level, Bill C-11, the government's amending legislation to replace the *Personal Information Protection and Electronic Documents Act* (PIPEDA) with the proposed *Consumer Privacy Protection Act* (CPPA), is intended not only to move Canada into the second-generation privacy law world, but also to ensure that our reformed federal law continues to meet the GDPR's adequacy (read equivalency) of protection requirement enabling unrestricted data flows between the EU and Canada.

However, Bill C-11 died on the order paper and Quebec's reform law, Bill 64, became the first Canadian second-generation law to be passed, in September 2021.[3] Drawing on numerous GDPR principles, Bill 64 arguably has "put a stake in the ground" for a new higher bar of privacy protections in the Canadian context.

So where does this leave the federal reform initiative and the issue of harmonization with Bill C-11's successor? Critics of Bill C-11 have suggested that it fails to achieve many of the standards of protection provided for in the GDPR.[4] If Quebec's new law sets a higher standard than Bill C-11, what does that do to harmonization within Canada? Also, as we know, other provincial reform initiatives are likely. Reports issued in Ontario and BC suggest that many of the Bill 64 precepts may find their way into the reform laws in those provinces.[5]

What is meant by interoperability, or harmonization?

Harmonization among privacy laws is not necessarily a requirement for interoperability. However, achieving elements of harmonization should result in substantial progress towards interoperability. Furthermore, it is fair to say that both harmonization and interoperability have the same objective – efficiency of application and compliance.

Interoperability means mechanisms that enable different regulatory or operational systems to work in alignment, even if not all elements of the systems are similar, or the same. Harmonization is the result of aligning regulatory or operational systems within their respective statutory rules, or through interoperability mechanisms outside of those rules, such as codes of practice or regulator guidance.

The Canadian experience makes clear that interoperability mechanisms can exist outside of the laws. The instances of significant cross-national privacy investigations in recent years are evidence that such alignment is being achieved in Canada.[6] A study of relevant rules in play both within Canada and internationally demonstrates that it is not necessary for such rules to be precisely the same. However it is also clear that consistency – or substantial similarity – of certain key elements is important.

---

[3] Amending the *Act respecting the protection of personal information in the private sector (Private Sector Law).*

[4] 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.

[5] See *Modernizing Privacy in Ontario,* Ministry of Government and Consumer Services White Paper, June 17, 2021 and *Modernizing British Columbia's Private Sector Privacy Law*, Report of Special Committee to review the Personal Information Protection Act, December 6, 2021.

[6] See for example, *Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Privacy Commissioner for British Columbia, Report of Findings*, April 25, 2019.

What key elements should be aligned?

1. Basic Premises

Firstly, a law's basic premises such as fairness and the status of the protections provided should be consistent. In this regard, the legal character of the privacy rights should have commonality. So for example, European law describes privacy as a fundamental human right,[7] a status which is echoed in Quebec's *Civil Code* and its *Charter of Human Rights and Freedoms*. Aligning with this status are the proposals in Ontario's White Paper and the BC Special Committee's Report that privacy should be recognized as a right.

However, in its initially proposed form, the federal CPPA did not include either a fairness principle or a statement of privacy as a fundamental right, although both of these premises have been urged on the government by the federal Privacy Commissioner in his commentary on Bill C-11.[8]

2. Definition of personal information

Secondly, the threshold definition of personal information, or as it is sometimes termed, "personally identifiable information", should be aligned. This definitional alignment includes both sides of the coin – what information is within the law's purview, typically described as "information about an identifiable individual" – as well as information that is outside of its application, in most instances termed "anonymous (or anonymized) information".

The inclusive portion of the definition is not controversial and is reflected in substantially similar language across both international and Canadian jurisdictions. Defining information that is outside of the law has been more difficult and often controversial. However there is a developing alignment. The GDPR and Quebec's new law define information anonymized information as information, outside of the law, that is made irreversibly non-identifiable.[9] The Ontario White Paper and the BC Special Committee Report take a similar approach.

Bill C-11's proposed approach is an outlier which likely will be adjusted to align with these other jurisdictions. The Bill's proposed category for information not subject to all of the law's rules is "de-identified information". While its terminology suggests that it should not be characterized as personal information (and therefore outside of the law), the definition contemplates potential re-identification and several provisions of the CPPA would continue to apply to such information.[10] Bill C-11's categorization is more closely aligned with the definition of de-identified (or "pseudonymized") information found in Quebec's new law and in the GDPR as well as proposed by the Ontario and BC reports. These definitions provide that information may be made non-

[7] GDPR, Recital 1.
[8] Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the *Digital Charter Implementation Act, 2020*, May 11, 2021 to the House of Commons Standing Committee on Access to Information, Privacy and Ethics.
[9] Quebec's definition provides further that anonymization must be accomplished in accordance with generally accepted best practices and with criteria and procedures prescribed by regulation; *Private Sector Law*, s. 23.
[10] See "Bill C-11 needs a comprehensive model for non-personal information", *Compliance Bulletin*, May 2021.

identifiable, and used for specified purposes not requiring the full protections of the law, but recognize that it can be re-identified by the addition of identifiers, either direct or indirect.

Achieving a clear understanding of the defined category of personal information is important not only for the basic premise of the subject matter of a law's application. It is important also to enable uses of information outside of the law, or requiring less rigorous protections, such as for purposes of innovation and research.

3. Scope of application

A third element of needed similarity is that of the scope of application. In this regard there is a somewhat substantial alignment among the Canadian current and proposed privacy law jurisdictions, in part dictated by their constitutional mandates. The federal law cannot apply to provincially-governed private sector employees. By contrast, each of the existing or proposed provincial laws would include this application. The federal jurisdiction is founded on the interprovincial trade and commerce power, which limits is application to the commercial activities of organizations, thus excluding many activities of charities and non-profits. However, the current and proposed provincial privacy laws include application to these organizations.[11]

One controversial area of scope is application to political parties. The current federal law, PIPEDA, and Bill C-11 do not include express application and the OPC has determined that it does not have oversight for any such application.[12] Quebec's Bill 64 makes provision for limited application of its private sector law, to provincial but not federal parties.[13] In BC, the OIPC has determined that it has jurisdiction over both provincial and federal parties.[14] Ontario's White Paper does not address the question.

4. Lawful data collection

Key substantive compliance items for lawful data collection constitute a fourth element of needed alignment. These encompass rules for valid consent, exceptions to consent, transparency requirements and accountability rules. Broadly speaking, these items should support the fairness premise of a law by requiring collectors of personal information to provide data subjects (i.e. individuals) with sufficient information to understand the implications of making their data available to a collector, including circumstances in which their consent is not required.

An important focus for potential differences in approach in respect of this element is that of disclosure of (and right to object to) decisions made by "automated decisions systems" (or "ADS"). This is a significant feature of the second-generation laws. Following the lead of the GDPR, all of the new or proposed Canadian laws address

[11] Application under Alberta's *Personal Information Protection Act* is limited to commercial activities carried on by such organizations, which is essentially the rule under PIPEDA; PIPA, s. 56.
[12] See: Letter regarding complaint against federal political parties, March 25, 2021.
[13] Bill 64, Title III.1, Protection of The Personal Information of Electors.
[14] See: Investigation Report P19-01 *Full Disclosure: Political parties, campaign data, and voter consent*, Feb. 6, 2019; Order P22-02, *Conservative Party of Canada, Green Party of Canada, Liberal Party of Canada, New Democratic Party of Canada*, March 1, 2022;

this issue. However differences in the specificity of disclosure and the rights of individuals to understand potential impacts and to object to an ADS decision are apparent.

5. Breach response procedures

Data breaches do not respect borders, whether inter-provincial or international. Consequently, it is critical for privacy regimes to have substantial alignment in their rules for breach response and reporting. This alignment will enable organizations to respond in a coherent and consistent manner in all jurisdictions affected by a breach and, importantly, for affected individuals to receive consistent notifications and benefit from protective actions irrespective of where they live.

Both the current federal law, PIPEDA, and the proposed CPPA provide a regime for notification of individuals and reporting to the OPC of breaches meeting the threshold of "real risk of significant harm to an individual", as soon as feasible. Alberta's *Personal Information Protection Act* breach response procedures are consistent. Quebec's breach response rules, new under its amended law, are also consistent with some distinctions in potential scope of application.[15]

Conclusion – Significant opportunity to align Canada's privacy laws

As can be seen, there are significant elements of alignment, or potential alignment, among the current and proposed second-generation privacy laws, both within Canada and internationally. As the "next batter up" among Canadian legislative regimes proposing reform, the federal government has a significant opportunity to crystallize alignment with its re-introduction of the CPPA. It will be closely watched to see to what extent a revised CPPA will respond to the critiques of Bill C-11 and the opportunities for consistency among key elements, as articulated in the amended Quebec statute and the directions indicated by the Ontario White Paper and the BC Special Committee's Report.

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

[15] In contrast to the PIPEDA and Alberta PIPA application to breaches involving *loss of, unauthorized access to or unauthorized disclosure of* personal information, the Quebec breach provision applies to the unauthorized *use of* personal information; *Private Sector Law,* ss. 3.5-3.8.