

Signs of things to come in Canadian privacy law reform and action to take now

Chantal Bernier and Sasha Coutu



Copyright 2022, The Sedona Conference and Chantal
Bernier and Sasha Coutu.
All rights reserved.

Signs of things to come in Canadian privacy law reform and action to take now

Chantal Bernier, National Practice Leader, Privacy and Cybersecurity, Dentons Canada

Sasha Coutu, Associate, Dentons Canada

The privacy regulatory framework is anything but static. Quebec's Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* received assent on September 22, 2021, introducing entirely new concepts in Canadian privacy law. The Bill was adopted unanimously, showing the level of political resolve to increase privacy protection. On November 17, 2020, the federal government revealed its direction in modernizing the *Personal Information Protection and Electronic Documents Act* (PIPEDA) through the defunct Bill C-11, the *Digital Charter Implementation Act, 2020*. The December 16, 2021, mandate letter to the Minister of Innovation, Science and Industry directs him to «*Introduce legislation to advance the Digital Charter, strengthen privacy protections for consumers and provide a clear set of rules that ensure fair competition in the online marketplace*». So, a new version of Bill C-11 will be back, in the hands of a different Minister than the one who introduced it. Ontario's White Paper, [Modernizing Privacy in Ontario](#), announces new private sector privacy law in Ontario, at times aligning with Bill 64 and former Bill C-11 but mostly going its own way. British Columbia and Alberta have also indicated they are looking to modernize their respective private sector *Personal Information Protection Act* (PIPA)

The tone is also changing around public sector privacy law: in British Columbia, Bill 22 – 2021: *Freedom of Information and Protection of Privacy Amendment Act, 2021* provides for relaxation of the prohibition for public institutions to store personal information outside of Canada, changing the playing field for private sector service providers. (See <https://www.dentonsdata.com/proposed-bc-fippa-amendments-would-loosen-requirements-to-keep-personal-information-in-canada/>.) Nova Scotia Premier Tim Houston made public his plans to grant order-making powers to the province's Information and Privacy Commissioner, in line with Canada's move towards an enforcement model to protect privacy.

To identify trends through adopted and announced Canadian privacy law reforms and plan accordingly, we have reviewed the legislative proposals, the related parliamentary debates and the reactions from industry and the privacy community. The purpose is to assess impact of legislative reforms to properly prepare or to propose alternative directions.

We observe these trends in Canadian privacy law reform and propose corresponding action.

1. Fragmentation of the Canadian privacy regulatory framework is a real risk

Innovation, Science and Industry Minister Champagne stated in March 2021 that the harmonization of provincial privacy laws is crucial for businesses and for investment in Canada. That is not the way legislative proposals are going. With a new private sector privacy law in Québec which aligns with Europe's *General Data Protection Regulation* (GDPR) rather than with Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA), former Bill C-11, instead, firmly going for the "Canadian way", a proposed "*made-in-Ontario*" private sector privacy law, and British Columbia as well as Alberta considering substantive amendments to existing privacy legislation, the risk of fragmentation is real and harmonization requires a deliberate effort.

It is understandable that each jurisdiction would want its own privacy regime, corresponding to its legal traditions and policy priorities. In addition, as the Ontario White Paper points out, PIPEDA's scope is limited to the information processed in the course of an organization's commercial activities. It leaves out

organizations such as charities, unions, associations and other non-profits with no other applicable privacy regulatory framework. This legal void has often been noted by provinces, which were able to fill this gap with their own private sector law. The Ontario's Information and Privacy Commissioner pointed out the need to close this gap in Ontario in relation to the privacy obligations of provincially regulated employers as well as political parties.

It is essential, however, that privacy regulation be coordinated, interoperable, across the country. An example of interoperability is section 3 of the British Columbia's *Personal Information Protection Act* (BC PIPA), which expressly excludes from its application the collection, use or disclosure of personal information if «*the federal Act applies [to it]* ». This would mean that an organization generally governed by PIPEDA for its operations across Canada, would only come under provincial privacy law in relation to the privacy rights of its employees. While it would have to contend with two privacy regimes, one for its commercial activities and another for its employee's personal information management, their respective scope of application would be clearly defined.

Action

Addressing legal voids without creating legal fragmentation must be a priority in modernizing Canada's privacy regulatory framework. The BC PIPA serves as a precedent to coordinate varying privacy regimes by avoiding overlapping scope.

2. The ombudsman model is out

Until now, all existing privacy legislation governing the private sector in Canada followed the ombudsman model rather than an enforcement model. Aligned with the intention of these laws, the role of the regulator under this model in the event of a complaint is primarily to mediate between individuals and organizations to resolve the dispute, and to make recommendations for organizations to improve compliance with their privacy obligations. Organizations fulfill their privacy obligations in the manner they deem operationally appropriate.

Research shows that the ombudsman model was chosen to allow an inexpensive, yet effective, out-of-court process that limits the burden on complainants and preserves the discretion of organizations in ensuring privacy compliance. At the time of adoption of PIPEDA, there was a concern that an onerous, prescriptive regime would hinder economic growth.

Since the adoption of PIPEDA, however, the Ombudsman model has become out of step with the reality of use of personal information in the digital economy particularly in relation to the power imbalance between individuals and organizations using their data and to the seemingly limitless profitability coming from the use of personal data. Legislators around the world, and now in Canada, call for commensurate powers for the regulators to represent individuals and for a level of monetary penalties that correspond to the level of profit.

It is clear from reading Bill 64, former Bill C-11 and Ontario's White Paper that Canada is determined to move from the ombudsman model to the enforcement model, and to complement this change with penalties that make the misuse of personal information as costly as its use is profitable. In fact, through Committee study, Bill 64 was amended to increase penal penalties to distinguish them from the administrative monetary penalties, hence confirming political will in that direction. The Bill grants the Commission d'accès à l'information ("CAI") the power to issue administrative monetary penalties (AMPs) – up to \$50,000 for individuals and, for organizations, the greater of \$10,000,000 or 2% of worldwide turnover of the previous

year. It also creates penal offences, where individuals may be subject to fines of \$100,000 (which were doubled by the Committee, from the initial \$50,000 proposed in the Bill) and \$25,000,000 or 4 % of worldwide turnover for an organization.

It is fair to expect that privacy legislation throughout Canada will follow that direction. The area begging for further debate is the process for recourse. Accessibility by individuals must be maintained and respondent organizations recourses must be fair. Regulators are fallible and increasing their powers calls for increasing oversight of regulators.

Action

Organisations must approach privacy compliance as a matter of ethics, consumer trust and significant financial risk. This entails the development of robust corporate privacy programs to both reduce the risk of contravention and demonstrate due diligence in the case of a challenge.

3. “Meaningful consent” will mean friction

Canadian privacy law is deeply rooted in a consent-based model. It should not be surprising. The right to privacy is defined by the Supreme Court of Canada in *R.v.Duarte* (1990) as the “*right of the individual to determine for himself when, how, and to what extent he will release personal information about himself*”. Consent expresses that determination.

When Bill 64 and former Bill C-11 were introduced, industry had hoped that legislators would have followed the GDPR’s lead to opt for a model less reliant on consent, allowing collection on the grounds of “legitimate interests”. The two bills have been criticized for overreliance on consent, being narrow and prescriptive in exceptions to the requirements to obtain consent.

Looking at how the proposed provisions of Bill 64 were amended and adopted through Committee, it appears there is limited openness to adapting the consent requirements to organizations’ operational realities. Exceptions to the requirement for consent were added in Bill 64 to allow the use of personal information to prevent and detect fraud or to evaluate and improve protection and security measures, as well as for the supply or delivery of a service or product requested by the person concerned. Proposed exceptions were kept for consistent use, use clearly for the benefit of the person concerned, or for study or research purposes or for the production of statistics where the information is de-identified.

But that is as far as the needle moved. The Ontario White Paper proposes an equally strict consent regime. Taking the position that “the *Bill C-11 proposals may not adequately protect Ontarians*”, the White Paper puts forward proposals to improve the obtention of meaningful consent while making consent more informed and preventing the exploitation of people’s data by organizations. The proposal, however, to provide for different “*authorities*” for the processing of personal information to reduce “*consent fatigue*” could be the avenue to introduce legal grounding akin to “legitimate interests”. But the White Paper also proposes to “*improve upon Bill C-11*” by excluding the possibility to act without consent even where consent is impracticable because the organization does not have a direct relationship with the individual.

Action

Achieving relaxation of proposed rules on consent will be difficult in the short term. Members of Parliament and Legislative Assemblies will be receptive to the position of their constituents – intuitively in favour of strict consent rules. While with time the illusory nature of strict consent requirements may become more apparent, for now, organizations should focus on compliant consent mechanisms that create minimal

friction either because they are user-friendly and engaging or because they are layered, providing the option to the user to exercise more or less granular consent. The “Accept cookies” and “Manage cookies” options are examples of that layered approach.

4. Transparency has reached a whole new level

Compared to consent, transparency is an easier way to empower individuals to control the use of their personal information. Privacy notices are the primary instruments by which organizations meet transparency obligations. A new level of transparency requirements has made its way to North America not via Canada, but via the far less privacy regulated United States, through the *California Consumer Privacy Act* (“CCPA”). This is indicative of the impact consumers have to influence privacy law. While Canadian transparency requirements create general obligations for organizations to make available information about their personal information management practices and, through individual access requests, to provide individuals access to their personal information, the CCPA grants consumers the “*right to know*” by requiring organizations, upon request from individuals, to disclose extensive information about their practices. As under Canadian law, this includes the categories and specific pieces of personal information they have collected on the consumer. In addition to Canadian law, it specifically requires disclosure of the categories of sources from which personal information is collected, specific business or commercial purposes for collecting the personal information, the categories of third parties with whom the personal information is shared and the categories of personal information that the business sells or discloses to third parties. This high level of disclosure requirements forms part of the context in which legislative proposals to modernize Canadian privacy law develop.

Through Committee study of Bill 64, the transparency requirements related to the disclosure of information were refined. Organizations will have to proactively, at the time of collection and upon request, inform individuals of the purposes and means of collection, of individual privacy rights, of the right to withdraw consent to the use or communication of the information, of the possibility that information could be communicated outside Québec and, where applicable, of the names or the categories of third parties to whom it is necessary to communicate the information (e.g., service providers)

New to Canadian law, Bill 64 requires transparency of use of automated decision-making systems (ADS). Individuals will have the right to know what personal information about them was used to make the automated decision, to have it corrected and to present observations to a person who is in a position to review the decision.

Former Bill C-11 had less prescriptive language, as is typical of the federal privacy law, and put forward slightly different disclosure requirements, while maintaining the current requirements. Organizations would have had to proactively disclose the type of personal information under their control and provide a “*general account*” of use, including how the organization applies the exceptions to the requirement to obtain consent, and uses of ADS. The duty to disclose transfers of personal information across provincial or national borders would have been enshrined in law but limited to transfers that “*may have reasonably foreseeable privacy implications*”.

Ontario’s White Paper’s proposal to ensure “data transparency” mirrors that of Bill 64 and Bill C-11 showing a consensus in privacy policy to broaden disclosure obligations as well as to increase requirements for clarity in relation to privacy notices to support consent.

Action

Organizations must update their privacy notices to include all the information required in every jurisdiction in which they operate. The focus on clarity and accessibility of language suggests having the legal drafts reviewed by the marketing team to remove the legalese in favour of user-friendly texts.

5. The right to data portability has been clarified

The technological challenges surrounding the implementation of the right to portability have been widely discussed, but definition of its scope also raises concerns. Committee study of Bill 64 brought forward clarification that in Québec law the right to portability will only apply to information provided by the individual and not to information about the individual *«created or derived from personal information about the individual»*. Former Bill C-11 may be interpreted to the same effect, applying the right to mobility to *“personal information that [the organization] has collected from the individual”*. Bill 64, however, may pave the way for greater clarity in legislating the scope of the right to portability.

The objective in recognizing the right to portability is to reinforce competition and empower consumers to have the ability to choose the organizations they conduct business with. Excluding from the right to portability information derived by the organization serves to both protect the intellectual property of the organization and the privacy of the individual.

Action

Hopefully, this amendment to Bill 64 will lead to similar clarification throughout Canadian law on the right to portability. On the part of organizations, implementation of the right to portability will require addressing, through guidelines to staff on the distinction between the information subject to portability and that which is not, and processes to respond to individual requests,

6. Privacy Impact Assessments (PIAs) requirements are on the rise

Bill 64 requires organizations to perform PIAs for any *“project of acquisition, development and redesign of an information system or electronic service delivery involving the collection, use, communication, keeping or destruction of personal information”*. This is a narrowing of the originally proposed requirement. PIAs are also required before communicating personal information outside Québec or communicating personal information without consent in the context of study, research or for the production of statistics. The Ontario White Paper also envisages PIAs asking whether Ontario should consider mandatory requirements for Privacy by Design practices or privacy impact assessments.

Former Bill C-11 did not include mandatory PIAs, but the Office of the Privacy Commissioner of Canada called for amendments to require *“privacy impact assessments on high-risk activities”*. The recommendation is most likely to be renewed in relation to the next version of Bill C-11.

PIAs are already required under some privacy legislation in Canada, for example, under Alberta's *Health Information Act*, and they are commonplace throughout the public sector at all levels of government. Organizations subject to the GDPR already have the obligation to proceed to a Data Protection Impact Assessment (DPIA) where the adoption of new technologies *“is likely to result in a high risk to the rights and freedoms of natural persons”*.

As the focus on accountability for privacy compliance increases, both in law and through the regulator's expectations, PIAs stand-out as demonstration of accountability and documentation of due diligence.

Action

PIAs are very helpful tools for organizations to assess privacy risk exposure, develop appropriate and proportionate safeguards and to routinely check their ongoing compliance in a planned and structured manner. They are inherent to implementing Privacy by Design and Privacy by default, two concepts becoming standards in privacy regulation.

It is fair to expect that requirements for mandatory PIAs for certain “high risk activities” will expand. Even where the practice is not mandatory, many organizations would gain in adopting a process to assess and mitigate privacy risks. Compliance assurance will increase, and due diligence will be documented to significantly buttress the legal position of the organization in the case of a challenge.

7. Anonymization will no longer remove data from the reach of privacy law

Currently, PIPEDA provides organizations with three options regarding the fate of information that is no longer required to fulfil intended purposes: destruction, erasure and anonymization. Exercising any of these options will result in transforming personal information into information that is no longer personal, considering that it no longer relates to an identifiable individual. As a result, it no longer comes within the ambit of privacy law.

That is still the case for the GDPR, but it is not where Canada is going.

Bill 64 regulates “de-identified” and “anonymized” information. Information is “de-identified” if it no longer allows the person concerned to be directly identified. It is “anonymized” if it irreversibly no longer allows the person to be identified directly or indirectly.

“De-identified” information remains personal information since it can still be traced to the individual through a second source. As is the case now, it is protected by privacy law.

The unprecedented move of Bill 64 is to regulate “anonymized” information. The original Bill required that the information be anonymized “according to generally accepted best practices.” Through Committee, the requirement was added that it be used “*for a serious and legitimate purpose subject to any preservation period provided for by an Act.*”

The policy behind the extension of privacy law to anonymized information rests upon a concern that, considering the volume of personal data on the internet and the capacity to match it, anonymization is more difficult or impossible to achieve. The philosophy behind the regulation of anonymized information rests upon the concept of “human data”: no longer attached to an individual but protected by a collective right to privacy, to regulate the use of information derived from humans.

Former Bill C-11 was guided by the concern that anonymization was no longer achievable. It introduced a definition of “de-identify” that corresponded to what would be considered as “anonymized” under Bill 64 and under any other privacy legislation, including the GDPR. The Bill would have imposed restrictions on the resulting information, while the same information is free to use anywhere else. The provision muddled the waters around the legal status of anonymized data and must be reworked in a new iteration of modernization of PIPEDA.

In contrast, the Ontario White Paper proposes to “*incentivize the use of anonymized data by removing it from privacy rules altogether.*”

Action

The use of de-identified and anonymized information is critical to progress in the understanding of society and of its phenomena, for the public good. In relation to Bill 64, it calls for the delimitation of the scope of “*serious and legitimate purpose*” broad enough to encompass the investigative and speculative nature of research and innovation. In relation to a new federal bill to modernize PIPEDA and to a bill to introduce private sector privacy law in Ontario, proposals regarding anonymized information will have to receive consideration enlightened by experts in the field with respect to the real risk of re-identification/

For organizations, internal guidelines will have to be developed to properly govern the methods of de-identification and anonymization and the use of the resulting information.

8. Rules on cross-border data flows will vary across the country

In existing Canadian private sector privacy laws, Québec and Alberta are the only two jurisdictions that explicitly impose conditions upon cross-border data transfers. Both expressly require comparable protection and Alberta also requires notification of individuals. At the federal level, the requirement for comparable protection is read into the accountability principle in relation to any transfer of personal information to a third party for processing and the obligation to notify individuals is read into the openness principle, as information material to consent.

Bill 64 introduces a new process.

While softened through Committee after much debate, Bill 64 was adopted with the requirement that any communication of personal data outside Québec be subject to a PIA for organizations to determine, prior to communicating the information outside of the province, that protection in the receiving jurisdiction would be “adequate” according to privacy principles.

Former Bill C-11, however, confirmed Canada’s direction to not create specific restrictions on cross-border data flows, save for the obligation that individuals be notified of interprovincial and international transfers, but only if the transfer may “*have reasonably foreseeable implications.*”, Commercial and technological reality is that, whether through cloud service providers or through trade, personal information crosses, at the very least, the Canada - U.S. border, as a matter of course. Through the new Canada-United States-Mexico Agreement (CUSMA), Canada has undertaken not to impose cross-border data restrictions except in limited cases which are justified by national interests. From former Bill C-11, it appears that the federal position is entrenched, reflecting commercial and technological realities.

Comparing these legislative proposals shows that political and economic differences drive legislative policy on this issue, and we are most likely to have one regime for Québec, and another for the rest of Canada. That being said, the determination of adequacy imposed by Bill 64 is akin to the existing obligation under PIPEDA for organizations to ensure, in any transfer, “a comparable level of protection “. Quoting the Office of the Superintendent of Financial institutions(OSFI), in its 2009 Guidelines for processing personal data across borders the OPC expects that, in transferring personal data abroad, organizations take into account “*potential foreign political, economic and social conditions, and events that may conspire to reduce the foreign service provider's ability to provide the service, as well as any additional risk factors that may require adjustment to the risk management program*”. This is not far from the PIA required through Bill 64.

The issue must also be considered through the lens of the so-called “Schrems II” judgment of the Court of Justice of the European Union of July 16, 2020. The Court put upon organizations the duty to ensure that cross-border transfer of personal data, including onward transfers such as through the storing in a US based cloud of European data by a Canadian organization, that the situation in the country to which the data is exported does not undermine the protection of the data.

Action

As consumers increasingly pay attention to where their personal information is stored, specifically due to the fear of access by local State authorities and lax cybersecurity laws abroad and considering the trend towards putting upon organizations the responsibility to assess equivalency of foreign privacy law regimes as well as privacy implications of cross borders transfers, organizations would be wise to develop internal processes and guidelines to manage this legal risk. The exercise implies a survey of all service providers to determine the countries in which they store data, an assessment of the data protection regimes in those countries and policies as to where the organization will accept data to be stored, or not.

The exercise could take the form of a PIA, satisfying Québec’s legal requirements and providing the organization with a clear view and direction on managing the risk of data storage abroad.

9. The use of artificial intelligence will come under increasing scrutiny and regulation

Automated decision-making systems (“ADS”), referring to the concept of leveraging the power of artificial intelligence to make decisions in varying contexts, such as to serve ads, to personalize services, or to assess various types of applications, is becoming more common, pushing the limits of existing privacy laws. Recent documentation of algorithmic manipulation of individuals sharpens the focus on ADS as a matter of democracy, fairness and privacy through the use of personal information without transparency.

Bill 64, former Bill C-11 and the Ontario White Paper all address ADS. The focus is on algorithmic transparency and algorithmic fairness.

To regulate the practice of using such technology, Bill 64 requires organizations to inform individuals of a decision based exclusively on automated processing, no later than at the time of informing the individual of the decision itself. In addition, individuals must be granted, upon request, access to the personal information used to render the decision, to the reasons and the principal factors and parameters that led to the decision and the individual must be informed of the right to have the personal information used to render the decision corrected. Individuals must also be given the opportunity to submit observations to obtain a review of the decision. Failure to meet these obligations can lead to an administrative monetary penalty by the CAI.

Bill C-11, while less exigent and merely creating transparency requirements, also sought to regulate the use of automated decision-making technology. Organizations, on request by individuals, would have been obligated to provide an explanation of the prediction, recommendation or decision resulting from the automated decision-making system and of how the personal information was obtained to make the prediction, recommendation or decision.

Ontario’s White Paper adds its own angle to the regulation of ADS, by addressing the risk of profiling and surveillance. Similar to Bill 64 and former Bill C-11, Ontario examines the scope and transparency of ADS, including the right for individuals to receive an explanation of the outcome of any application of ADS in relation to them.

The prevalence and impact of ADS, which is now under unprecedented media focus, is most likely to attract regulation on a wider scale, through and beyond privacy law.

Action

The OPC already inquires, as relevant, about algorithmic bias, asking organizations how they check their ADS configuration to avoid bias. In the face of increased scrutiny on ADS, organizations should keep a clear record of the data they use through ADS and develop proper disclosures to be transparent about ADS. Balancing transparency and the confidential nature of the specific logic of ADS can be reached following the model of the GDPR: organizations are required to provide “*meaningful information about the logic involved.*”

10. **There is room for change in a new version of Bill C-11**

Bill C-11, the *Digital Charter Implementation Act*, died on the Order Paper after limited debate in the House of Commons and is now in the hands of the same public servants, the same government, but with a different Minister than the one who tabled it. The new Minister is enlightened by the leading reactions to the proposed provisions. Those reactions show the main points of pressure to be addressed by government in its preparation and eventual debate of a new version of the Bill. In particular,

- Fear of surveillance. Early on during the first debates on Bill C-11, the Conservative Party of Canada (“CPC”) denounced what it saw as inaction from the Government of Canada in response to mass surveillance and behaviour manipulation by the industry and the lack of enforcement for privacy violations. Since then, The House of Commons has been concerned with alleged surveillance around the use of cellphone data and revelations have emerged on manipulation of opinion through social media. The issue is likely to gain increased prominence.
- Disagreement on consent: The CPC also requested that individuals be provided with the right to object to the sale of personal information, following the model of the CCPA. The New Democratic Party (“NDP”) joined the CPC in expressing concerns regarding the proposed exceptions to consent related to commercial uses of personal information. Two particular areas of concern were identified; first, the authorization to collect or use personal information without knowledge or consent in “the public interest” and, second, the open-ended exception to the collection or use of personal information without knowledge or consent for “business activities” that are prescribed by the regulations. With the former, the concern expressed by the CPC was specific to the conflict of interest that could arise, for example, if an organization mandated under federal or provincial law or by contract with a government was to process personal information for such purposes. The Green Party also expressed concerns about the provisions on consent raising the specific issues of the lack of provisions regarding the protection of minors.
- Criticism of the enforcement model. The NDP and the CPC expressed concerns about the lack of efficient enforcement, which aligns with the OPC’s reaction to the Bill. Specifically, the enforcement process was criticized as overly burdensome and “unusable” for individuals to seek quick compensation in court for privacy-related violations.
- Confusion about de-identified information. Consistent criticism has emerged around former Bill C-11’s provisions on de-identified information. Because the definition equates that of “anonymized” information under all other privacy laws, and subjects it to restrictions not applicable to anonymized information under any other privacy law, the wording of Bill C-11 would have had the unintended

consequence of uniquely removing access to anonymized information for organizations governed by the federal legislation. Re-wording Bill C-11 here is critical and will be claimed.

The Government defended the Bill as one that is balanced, allowing for flexibility while leveraging technology-neutral mechanisms.

It remains to be seen whether the harsh criticism from the OPC, including the statement that Bill C-11 was a step back from the current protections under PIPEDA, will survive the arrival of a new Privacy Commissioner in June at the latest. That being said, the OPC's 60 recommendations submitted to Parliamentary Committee regarding Bill C-11 cannot be ignored.

One thing is sure: Canada is under pressure to update its federal privacy law. Canada hopes to maintain its adequacy finding from the European Commission that allows organizations coming under PIPEDA to receive personal data from the European Union without further authorization. This requires updating PIPEDA to raise the bar to a level closer to that of the GDPR, particularly in regard to enforcement mechanisms. In addition, public concern with respect to online privacy is growing, leading to the general distrust that paves the way for disinformation. Finally, Canada must remain competitive with a privacy regime that properly protects individual rights while allowing the use of data for the public good.

Action

Former Bill C-11 should serve as a "dry-run" to modernize the federal privacy framework taking into account the reality of new privacy risks and new opportunities in the use of data for good.