David Young Law
Compliance Bulletin

December 2021

2021 Privacy Recap – Focus on reform and digital data

The past year has seen developments advancing the focus of privacy laws with significant potential impacts on technology and data. Most importantly, initiatives for reform at both the federal and provincial levels have progressed, with the objectives of both strengthening protections for personal information and facilitating innovation.

Heightening the regulation of digital data also has been pushed forward by the COVID-19 pandemic, with a surge of technologies playing a critical role in enabling health care, economic resilience, and social interactions to continue to function, responding to the new realities.

In addition to the privacy reform developments, two cases of note have focused on digital and technology issues.

Privacy law reform – second-generation privacy laws

This thrust of reform has been characterized as enacting "second-generation" privacy laws - which in large part take their inspiration from the EU's *General Data Protection Regulation* (GDPR). The GDPR, which became law in 2018, chronicled a more rigorous and potentially far-reaching level of mandatory privacy law than the "first-generation" laws, of which the EU's 1995 *Data Protection Directive* and Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) were representative.[1]

The second-generation laws are oriented to digital data and are anchored in a user "rights" framework with strong protections for information processed by artificial intelligence and other automated decision systems (ADS), requiring organizations to proactively notify individuals of such processing and to provide the ability to object.

While adopting enhanced protections for data used in ADS, the second-generation laws also seek to facilitate innovation, by providing for technology-friendly functions for the processing of data without consent, such as where it has been de-identified, or in circumstances where meaningful consent is understood but may be difficult to obtain.

To backstop the proposed enablements for innovation, the new laws are predicated on privacy as a human right. Enforcement of this right is supported by enhanced accountability including requirements for privacy by design as well as privacy impact assessments (PIAs) for high-risk projects.

Finally, the second-generation laws provide for the imposition of significant monetary penalties for non-compliance.

[1] The GDPR is providing inspiration for privacy law reform worldwide, including in North America, for example, the *California Consumer Privacy Act*.

Quebec Bill 64 becomes law

Firstly, and most significantly, Quebec's legislation updating its *Private Sector Law*[2], Bill 64, was passed on September 21, for the most part to come into effect two years hence.

The Bill 64 amendments enact what may be characterized as a second-generation law, taking Quebec's *Private Sector Law* to the level of more rigorous compliance requirements, consistent with the GDPR.[3] They include provisions addressing transparency, requirements for clear and informed consent, notification of profiling and automated processing, rights to de-indexing (i.e. right to be forgotten) and data mobility, and a right to present objections to automated processing. The amendments also include requirements to conduct PIAs with respect to new electronic processing projects and to follow privacy by design principles.

The amended private sector law also includes rules facilitating innovation, such as permitting use of de-identified personal information for internal research.

Federal privacy reform

The federal government also is seeking to update PIPEDA with a second-generation law, the *Consumer Privacy Protection Act* (CPPA), again with a view to the GDPR. The CPPA was to be enacted under the now-defunct Bill C-11 – the government's proposed *Digital Charter Implementation Act, 2020*.

The CPPA adopted the GDPR's requirements relating to transparency for individuals affected by automated processing by requiring disclosure of such methodologies and providing for a right to receive an explanation of any prediction, recommendation or decision made by such processing. However the CPPA did not contain any requirement to proactively notify individuals, nor the right to object, as is contemplated in the GDPR and the Quebec amendments.

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 the conundrum that innovation requires access to large amounts of personal data. Bill C-11 sought to respond to this dictate through expanded exceptions to the consent requirement, including for a new category of "business activities", as well as for "socially beneficial activities" and for de-identified information.

A significant and potentially privacy-limiting exception was the proposed new category of uses for business activities where an organization does not have a direct relationship with an individual and where obtaining their consent would be impractical. This exception – which has been subject of criticism – could have potentially extensive impact for digital data uses including profiling and algorithmic assessments such as for insurance and financial risk purposes.

[2] *Act respecting the protection of personal information in the private sector*.
[3] For a discussion of the amendments, see *Compliance Bulletin,* October 2021.

Commentaries regarding the Bill have variously either supported its thrust or leveled some strong criticisms. Most significantly, in its May 2021 Submission to the Parliamentary ETHI Committee,[4] the Office of the Privacy Commissioner delivered a severe critique, arguing that in its then form the Bill would represent a step back overall for privacy protection in Canada.

The OPC argued that although seeking to address digital privacy issues, the Bill proposed to do so in ways that would be less protective than laws of other jurisdictions, such as the GDPR. Specifically, in the OPC's view, its provisions would give individuals less rather than more control over their data; furthermore, the increased flexibility for organizations to use data without consent would not come with additional accountability.

Probably the OPC's most overarching criticism was the Bill's failure to enshrine privacy as a human right, arguing that privacy interests should always trump commercial interests instead of in effect being balanced against one another.

The federal Innovation Minister has re-iterated the government's commitment to introduce an updated version of the CPPA in 2022, indicating that feedback from commentators is being considered and potentially will be reflected in a revised Bill.[5]

Ontario White Paper

In addition to the now-adopted Quebec law, other provinces are considering reform of their first-generation laws incorporating precepts envisaged for second-generation privacy laws, as well as, in Ontario's case, the adoption of an entirely new stand-alone private sector law.

Ontario's vision for a second-generation law was set out in its White Paper, *Modernizing Privacy in Ontario*, proposing a private sector privacy law, published in June.

Ontario's proposals would implement privacy as a fundamental right, introduce safeguards for data use in automated processing, provide protections for children, update consent rules to respond to the modern data economy, and promote responsible innovation through, for example, clearly defining the categories of de-identified and anonymized data.

Important corollaries to the introduction of an Ontario law would be the extension of privacy protection to private sector employees, currently not covered by any privacy law, and the clearer application of privacy rules to the not-for-profit and charitable sectors.

BC Special Committee Report

In February 2020, the BC legislature appointed a Special Committee to review the province's *Personal Information Protection Act* (BC PIPA). Following an extensive public consultation, the Committee issued its Report, *Modernizing British Columbia's Private Sector Privacy Law*, on December 6, 2021.

[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] "Champagne promises updated privacy legislation in new year", *The Logic*, December 6, 2021.

The Committee's Report articulated a view for a second-generation PIPA. As guiding values, it set forth establishing privacy as a right, adaptability with new technologies, supporting innovators, and consistency with provincial, federal, and international legislation.

The Committee also recommended strengthening the Commissioner's enforcement powers, including administrative monetary penalties sufficient to deter non-compliance.

The Committee addressed special protections for sensitive categories of information, including relating to children and youth, biometrics, political views, religion, sexual orientation, and medical information, and recommended that PIPA should be amended to require explicit consent and specific data handling practices for such sensitive data, including with respect to social media interactions with young people.

Alberta PIPA consultation

Lastly, over the summer, in response to a November 2020 letter from the Alberta Information and Privacy Commissioner, Jill Clayton, proposing changes to update the province's *Personal Information Protection Act* (Alberta PIPA), Service Alberta undertook a consultation.

Commissioner Clayton had advanced her view that Alberta PIPA needs updating to adapt to accelerated digitization across society, particularly in light of the COVID-19 pandemic, and enhanced societal expectations relating to access to information and privacy rights. Contexting her recommendations, Commissioner Clayton referred to the other second-generation privacy law initiatives across the country as well as the GDPR.

No report on the Alberta consultation has been released as yet.

Clearview AI and the regulation of biometric data

Two cases involving digital data, one a regulatory investigation and the other in the courts, may be noted.

In a decision released in February,[6] the federal Privacy Commissioner and his provincial counterparts in Quebec, Alberta and B.C. ruled that Clearview AI's creation of a database of photographs of individuals taken from the Internet for law enforcement purposes contravenes Canada's privacy laws. Clearview's business model involves "scraping" photographs of individuals from the Internet and providing them, together with other identifiable data, to police forces to aid in their investigations. During 2019 and 2020 a number of Canadian law enforcement agencies, including the RCMP, used the service, on a free, trial basis.

The Commissioners found that the information at issue (facial biometrics) was sensitive and that Clearview AI's mass and indiscriminate scraping of these images from millions of individuals, including children, and the subsequent use and disclosure of that information for its own commercial purposes – unrelated to the purposes for which the images were originally posted, and potentially, to the users' detriment and risk such as through

[6] *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta;* PIPEDA Report of Findings #2021-001, February 2, 2021.

prosecution or misidentification, was not an appropriate purpose under the privacy laws and therefore failed to meet the laws' basic precondition for acceptability.

Further to the decision in the case, the federal Commissioner in a separate investigation concluded that the RCMP contravened the federal public sector law, the *Privacy Act*, when it collected information from Clearview, stating that a government institution cannot simply collect personal information from a third party agent if that third party's collection was unlawful in the first place.

The Commissioner's investigation highlighted other concerns related to the use of novel technologies.

It found that Police use of facial recognition technologies, with its power to disrupt anonymity in public spaces, and enable mass surveillance, raises the potential for serious privacy harms unless appropriate protections are in place.

The Commissioner stated that Canadians must be free to participate in the increasingly digital, day-to-day activities of a modern society without the risk of their activities being routinely identified, tracked and monitored.

As a result of their investigation, the federal and provincial Commissioners have launched a consultation on draft guidance to help police ensure any use of facial recognition technology complies with current laws and minimizes privacy risks.

The Commissioners also stated their view that it is necessary to carefully consider issues related to facial recognition technology more generally as Canada looks to modernize federal privacy laws. They stated that currently the technology is regulated only through a patchwork of statutes and case law that, for the most part, do not specifically address the risks posed. This creates room for uncertainty concerning what uses of facial recognition may be acceptable, and under what circumstances.

Most recently, on December 14, the BC Commissioner issued an Order requiring Clearview to cease its facial recognition services in that province and to use its best efforts to cease collecting images of BC residents and delete those which has collected previously, measures which were recommended in the Joint Investigation Report but which Clearview had refused to adopt.

Google Reference Case

In its recent ruling regarding the jurisdiction of the federal private sector privacy law, PIPEDA, over Google's search engine operations, and the issue of whether PIPEDA includes a "right be forgotten", the Federal Court ruled that PIPEDA does apply, including with respect to the indexing of search results. [7]

Google's submissions had included the argument that notwithstanding the commercial nature of its overall search engine business, involving creating profiles of users and using these profiles for targeting ads, the specific functions of collating and organizing information collected, at no cost, from content providers/publishers across

[7] *Reference re Subsection 18.3(1) of the Federal Courts Act,* 2021 FC 723 (CanLII) (*Google Reference* case).

the Internet, did not constitute a commercial activity subject to PIPEDA.[8] The *Google Reference* case did not however address the broader constitutional question of whether the application of PIPEDA to Google's search engine operations contravenes the right to free speech protection under the *Charter of Rights and Freedoms*. Google has appealed the decision on this point specifically, arguing that PIPEDA's journalism exemption, in paragraph 4(2)(c), which it had submitted as an alternative basis for the non-application of the law, should be interpreted in the context of the freedom of speech right. The court had declined to do so.

Conclusions

Several conclusions can be identified from the privacy reform and case law developments of 2021.

Firstly, in light of the Quebec amendments, now law, and the other provincial reform initiatives, it is reasonable to expect that there will be significant alignment among all of the provinces that have or are expected to have private sector privacy laws, as well as with the revised federal Bill – pointing to a clearer adoption of the second-generation law model across Canada, with particular focus on digital data and technology.

Secondly, a rights-based model for privacy protection will be an integral aspect of the second-generation laws, with particular impact on transparency for automated processing of data.

Finally, collection of sensitive information will be subject to heightened scrutiny and procedural requirements, and potentially specific rules in the case of facial and other biometric information.

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

[8] The OPC has stated its view PIPEDA that applies to indexed information as is provided within search results; see *Draft Position on Online Reputation,* Jan. 26, 2018. Under Bill C-11, a limited right to be forgotten, extending only to information collected directly from an individual, was expressly provided for.