David Young Law
Compliance Bulletin

December 2020

2020 Privacy Recap – Some Significant Events

The past year has seen a number of diverse but significant developments on the privacy front – ranging from legislative reform to COVID response initiatives. A number of "moving pieces" are in play and where they all settle will impact on several levels well into the future. The following commentary highlights the main developments.

Privacy law reform

Reform of Canada's privacy laws was the central development to note. The federal government and three provinces – B.C., Ontario and Quebec - either introduced amending legislation or initiated reviews or assessments of current or potential new laws. As well, the federal Office of the Privacy Commissioner conducted a consultation into the impact of artificial intelligence on privacy, with a view to legislative reform. Finally, Elections Canada undertook a consultation for purposes of its report on the 2019 federal election, addressing political communications in the digital age, that focused in a significant way on the role of personal information collection within the electoral process and in particular by political parties.

Bill C-11 – Consumer Privacy Protection Act

On November 17 the federal government introduced its long-awaited legislation to reform Canada's private sector privacy law, PIPEDA.[1] By Bill C–11, the government proposes to replace PIPEDA with a new act, the *Consumer Privacy Protection Act*, and to enact a separate law, the *Personal Information and Data Protection Tribunal Act,* to create a quasi-judicial tribunal to impose monetary penalties and rule on appeals from matters determined by the federal Privacy Commissioner. [2]

In many respects, the CPPA achieves what might be characterized as "a fine balance" between a GDPR-like statute and PIPEDA'. Most significantly, the CPPA retains PIPEDA's ten *Fair Information Principles.* However it adds significant express GDPR rights, including the right to be forgotten, the right to portability, and the right to be informed of the implications of automated processing.

The CPPA adopts an enforcement regime that is very GDPR-like – providing for significant potential financial penalties[3] married to an order-making power for the OPC.

Significantly, the CPPA retains consent as the key control right for individuals with respect to their personal information. By contrast, the GDPR stipulates that personal information must be processed lawfully, providing consent as only one of several bases for lawful processing.

---

[1] *Personal Information Protection and Electronic Documents Act.*

[2] *Digital Charter Implementation Act*,

[3] Administrative monetary penalties (AMPs) of up to 3%, and fines of up to 5%, in both cases, of worldwide sales.

Seeking to address circumstances where express consent may be either difficult to obtain or not appropriate, the CPPA includes expanded exceptions to the consent requirement, including for designated "business activities", "socially beneficial activities" and de-identified information. While these exceptions arguably derogate from the goal of enhancing the control that individuals have over their information, they are seen as facilitating the dynamics of collection and use of personal information in circumstances where consent would be understood and therefore unnecessary to address, as well as encouraging innovation.

In addition to the new consent exceptions, the CPPA provides for the establishment of codes of practice and approvals of the Commissioner by which organizations can have their procedures and policies certified, potentially enabling new, innovative models for privacy compliance.

Quebec Bill 64

In June, Quebec also introduced legislation to update its private sector privacy law,[4] arguably anticipating the PIPEDA reform initiative. Bill 64 follows more closely the GDPR's prescriptive approach, but similar to the CPPA includes the new privacy rights of data portability, the right to be forgotten and algorithmic transparency. [5]

Bill 64 proposes new rules including a requirement to conduct privacy impact assessments for information systems involving the processing of personal information and for any transfer of information outside of Quebec unless the privacy rules in the receiving jurisdiction have been approved as equivalent to those of Quebec.

The new law would impose significant financial penalties along the lines of the levels proposed in Bill C-11 – AMPs of up to 2 % of worldwide sales and fines of up to 4%.

Ontario consultation regarding a private sector privacy law

In August the Ontario government undertook a consultation to consider the adoption of a private sector privacy law for Ontario. The government indicated that any such law would address many of the issues now reflected in the federal PIPEDA reform initiative. Also on the table will be privacy protections to Ontario-based private sector employees and extension of privacy obligations to charities, not-for-profit organizations and political parties, which are not addressed explicitly under the federal privacy law.

B.C. PIPA review

Earlier in the year, the B.C. legislature commenced a review of the province's *Personal Information Protection Act* (PIPA). In its submission to the Special Committee conducting the review, the Office of the Information and Privacy Commissioner for B.C. identified three areas in which it is looking at reforms, specifically, privacy obligations of organizations; privacy rights of individuals; and oversight authority of the Commissioner. Within these broad areas, the OIPC focussed on mandatory breach notification for organizations, enhancing the role of consent, transparency of automated processing, providing for data portability and the right to be forgotten, and

[4] *An act respecting the protection of personal information in the private sector.*
[5] *An Act to modernize legislative provisions as regards the protection of personal information.*

strengthening the enforcement powers of the Commissioner, specifically the power to impose significant monetary penalties.

The OPC's AI consultation

The week prior to the tabling of Bill C-11 the federal Privacy Commissioner released his report addressing regulatory reform in relation to artificial intelligence and automated processing.[6] This consultation, undertaken early in 2020, specifically focused on potential amendments to PIPEDA to address the regulation of AI and set forth proposals for comment. The OPC received submissions commenting on its proposals from stakeholders including industry, technology experts, and civil society groups.

The Commissioner's recommendations set forth two explicit rights with respect to automated processing – the right to a meaningful explanation of automated processing affecting individuals, and the right to contest automated decisions. To be noted, the CPPA adopts the first but not the second of these rights.

The CPPA adopts the GDPR's impactful requirements relating to transparency for individuals affected by automated processing by requiring disclosure of such methodologies and providing an individual the right to receive an explanation of any prediction, recommendation or decision about them. However the CPPA does not contain the correlative express right to object to an organization's using such automated processing/decision-making, as is provided in the GDPR and addressed, differently, in Quebec's Bill 64.[7]

Election Canada's consultation regarding political communications in the digital age

As part of its follow-up analysis of the 2019 election, Elections Canada published a consultation document, focusing on the changes in political communications over the past twenty years and the privacy implications of such changes. It noted that communications around elections — and in general — are increasingly digital, taking place through diverse formats. Many of these are enabled by big data and are highly targeted.

Background to this consultation is the view of many commentators that the regulatory regime addressing elections and oversight of political communications under the *Canada Elections Act* is largely out of date and is not responsive to the new and evolving idioms of digital advertising and social media communications.

Highlighted by Elections Canada in relation to this deficiency is the lack of effective privacy oversight of political parties and the organizations and consultants that work for them, enabling the largely unregulated collection and use of voters' personal information in connection with elections and in political issue communications more broadly.

The three areas of focus identified in Election Canada's consultation document were: political communications generally; social media's role in elections; and the application of privacy laws to political parties and other

[6] *A Regulatory Framework for AI: Recommendations for PIPEDA Reform*, Office of the Privacy Commissioner, November 2020.

[7] Quebec's Bill 64, while not providing for an express right to object permits affected individuals to submit observations and require a re-assessment of any decision made by such system.

political actors. Arguably, these areas represent the most critical issue areas for enhancing regulatory oversight of political communications in the new digital media environment, leading potentially to the extension of privacy laws to political parties.[8]

Facebook – intersection of privacy compliance and competition law

In a landmark conclusion to its almost two-year long investigation into the Cambridge Analytica data debacle, the Competition Bureau announced in May that Facebook had agreed to pay a $9 million dollar administrative monetary penalty.[9]

The announcement is exceptional on several accounts. Firstly, it represents the largest fine imposed in Canada to date for privacy noncompliance. Secondly – and importantly – it represents the first active foray by the Bureau into the digital data space signifying, potentially, an expansion of regulatory focus for privacy compliance, from the Office of the Privacy Commissioner, to now include the Bureau.

The OPC together with the B.C. Commissioner had conducted an in-depth investigation of the Facebook/Cambridge Analytica revelations, resulting in their *Report of Findings*, in April 2019 specifically identifying failures in regards to user consent, security and accountability. The Report set out recommendations for Facebook to bring its procedures into compliance. Facebook disagreed with the Report's findings and notified the OPC that it would not be adopting the recommendations.

In February, the OPC filed an application in the Federal Court seeking an order requiring Facebook to comply with the Report's recommendations.[10] In response, in April, Facebook moved to challenge the OPC's application through judicial review.[11]

The sum result – to date – is that while refusing to comply with the privacy regulators' requirements for compliance, and challenging the OPC's right to seek an order compelling such compliance, Facebook has agreed to a monetary penalty close to the maximum provided for under the *Competition Act*.[12]

COVID-19 privacy impacts

Distinct from the explicit privacy law developments mentioned above – but also with potentially equivalent long-term impact – are the privacy implications of digital data driven by the COVID-19 pandemic. Apart from health care management issues, privacy implications relevant to remote medicine, work, education and

[8] A signal omission in Bill C-11 is that of expressly extending privacy law to political parties and their related actors, urged by among others the parliamentary Committee on Access to Information, Privacy and Ethics.
[9] *Consent Agreement between the Commissioner of Competition and Facebook, Inc.*, dated May 8, 2020.
[10] Pursuant to ss. 14 and 16 of PIPEDA.
[11] Facebook sought the Court's indulgence in failing to meet the 60-day deadline for filing an appeal which it had exceeded both in respect of the *Report* and the court application.
[12] The penalty, while significant, pales in comparison with those proposed under the CPPA and Quebec's Bill 64, ranging up to the greater of $25,000,000 and 5% of worldwide sales.

shopping abound including surveillance considerations, screening of employees, and generally, the burgeoning collection of data inherent in electronic interactions.

On the public health level, information about individuals, both specific and aggregate, is understood to be a critical tool in identifying risk centres and taking protective measures. Major new initiatives have been undertaken by public health authorities, health research agencies, and statistics bodies to collect, analyze and report publicly on the incidences and impacts of the virus - across populations groups, geographically and within industry sectors. A significant hurdle in such data analysis work is the difficulty of obtaining patient-level information with sufficient identifying characteristics to make it useful for research and development of public policy. In this regard, focus has been placed on anonymization tools and privacy-protective methodologies as well addressing legislative reform to enable more efficient and rapid data analysis from sources across the health sector.

Within the delivery of care spectrum, virtual and remote functionalities have seen wide adoption. These care models raise numerous privacy issues including unauthorized recordings, data sharing, secondary data uses, increased scope for "snooping", and the security risks posed by expanded electronic health record databases. The shift to remote care and digitization of health information was well underway prior to the pandemic but clearly now has realized an irreversible leap forward. However the privacy modalities supporting this shift to digitization of health care lag. For example, facilities for direct patient access to their electronic health records is limited or not even available in many parts of Canada.

COVID Alert App

Arguably a disappointment in the data-driven initiatives responding to the pandemic has been the COVID Alert "notification" app, promoted by the federal government, adopted in nine provinces and territories, and approved by privacy regulators.[13] The app was intended as a digital substitute for analog (or manual) contact tracing. Google and Apple, the tech companies that developed the app, have described it as a supplement to offline contact tracing. However, to address privacy concerns, the app collects no identifiable information regarding users downloading it or notified users.

The app is entirely voluntary – a user who tests positive is not required to register their status with the app, although they are encouraged to do so. Furthermore, other app users who are notified if a positive-testing user does input that information are not required to have themselves tested or otherwise notify the public health authorities.

Challenges facing the app include the fact that non-app users may be a significant segment of the population. The technological limitations of the app restrict its use to only late-model mobile phone owners. It can be

[13] Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness.

reasonably assumed that such users do not include many members of lower-income groups and other at-risk persons such as seniors.

In Ontario, the app has been used to notify others by about 4.5% of those who have tested positive. The app's limited data utility for broader public health objectives, such as identifying hotspots, leads to the question of whether adopting digital tools for pandemic response should always be trumped by privacy concerns.

Remote work, school, shopping

Privacy implications relevant to remote medicine, work, education, and shopping include surveillance and the burgeoning collection of data inherent in electronic interactions. Transparency – meaning clear notification to users – regarding collection, use and disclosure, adopting data minimization principles, and ensuring that all data use adheres to a "reasonableness" criterion are just some of the requirements that must be addressed.

Potential unauthorized secondary uses – such as unrelated workplace purposes, data profiling or future marketing require particular attention. In this regard, organizations using remote tools have learned that they must review carefully the privacy policies of their service providers and delete permissions for information use not directly related to providing the specific service.

Conclusions

It is fair to say that the privacy developments of 2020 will provide a new framework of "guardrails" for privacy standards and expectations that will impact at several levels well into the future.

The reforms to Canada's privacy legislation will set the rules for data use and accountability over the next decade if not longer.

All of the instances of new or expanded data use in responding to the pandemic entail more extensive – or new – modalities for collecting, using and disclosing personal information, in most instances relying on electronic databases that collect and retain information as their default setting. Clearly, interactions are now being "documented" electronically, and potentially retained for future use, that did not occur prior to the pandemic, leading to new increased privacy compliance issues and likely regulatory scrutiny.

The overlay of the pandemic in a year in which significant legislative reform is in play, while coincidental, is propitious and will make for an interesting 2021.

For more information please contact:
David Young 416-968-6286 david@davidyounglaw.ca
Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.