David Young Law
Compliance Bulletin

December 2022

Privacy 2022 Recap – legislative reform and other developments

The past year has seen a number of significant privacy-related developments, including the continued march toward legislative reform, a new federal Privacy Commissioner, the extension of privacy law to federal political parties in one provincial jurisdiction, and a significant limitation on the potential future scope of the invasion of privacy tort.

Federal legislative developments – Bill C-27

On June 16 the federal government introduced Bill C-27, its revised proposed new private sector privacy legislation – the *Digital Charter Implementation Act, 2022* – essentially an updated *Consumer Privacy Protection Act* (CPPA) and the *Act to establish the Personal Information and Data Protection Tribunal* plus a new proposed law, the *Artificial Intelligence and Data Act* (AIDA).

The Bill constitutes a revised version of former Bill C-11, introduced in November 2020 as the government's initial foray into the realm of privacy reform. Bill C-11, amending the current federal privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), died on the order paper with last fall's election.

Bill C-27 incorporates a number of significant adjustments relative to Bill C-11, responding to stakeholder input including from the former Privacy Commissioner, Daniel Therrien.[1] However, it does not include other substantive changes proposed by the former Commissioner, civil society groups and others, in particular the recognition of privacy as a fundamental human right. Nor does it extend express application to political parties, also recommended by the former Commissioner.

In particular, the Bill includes a "legitimate interest" exception to consent along the lines of the EU's *General Data Protection Regulation* (GDPR), protections for children and youth, clear exclusion of anonymized information from the law but recognition that information that simply has direct identifiers removed (de-identified information) remains subject to the law, confirmation of the existing, established regime for application of privacy law to charities and other non-profit organizations, greater flexibility for the Commissioner in conducting investigations, and broadening the expertise base and authority of the proposed Tribunal.

Other criticisms of the Bill include its failure to recognize the privacy risks to groups, the need for greater accountability provisions Including requiring privacy assessments for invasive technologies, privacy by default, additional rigour surrounding cross-border data flows, and a more comprehensive regime governing third party data processors/service providers.[2]

---

[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] See for example, Not Fit For Purpose - Canada Deserves Much Better - Centre for Digital Rights' Statement on Bill C-27 Canada's *Digital Charter Implementation Act, 2022*, October 28,2022.

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

Oversight of high-risk artificial intelligence systems

A potentially significant provision of Bill C-27 is the proposed enactment of the AIDA, intended to establish an oversight regime for "high impact" artificial intelligence systems, with a view to preventing their potential harmful effects such as bias, physical and psychological health consequences, and economic loss.

The AIDA is intended to apply to AI systems "related to human activities" that qualify as "high impact" – a key term which will be defined in regulations. Organizations operating such systems will be required to conduct risk assessments and undertake measures to mitigate risks identified by such assessments. The focus of the legislation will be in effect to regulate AI systems that have potentially significant negative impacts.

The proposed AIDA has been criticized as a "shell" of a law because many of the substantive provisions are not stipulated in the Bill but are to be defined by subsequent regulations including most importantly, what is to be considered "high impact". Another criticism is that regulation under the AIDA should not be the responsibility of Innovation, Science and Economic Development Canada (ISED) and the proposed new Data Commissioner who will be appointed by and report to its Minister since it is also the arm of government responsible for writing the legislation.[3]

Bill C-27 has been tabled for second reading in Parliament but is yet to be referred to committee where potential amendments may be introduced. Committee hearings will commence only in the new year with passage of the Bill therefore unlikely before the second quarter of 2023.

Law 25 amending Quebec's Private Sector Act

Some of the provisions of Quebec's legislation updating its *Private Sector Law*[4], previously known as Bill 64, came into force on September 21. Specifically, the requirement for organizations to appoint a privacy officer and the requirements for breach response, broadly analogous to those in force under PIPEDA and Alberta's Personal Information Privacy Act (Alberta PIPA), are now law. The balance of the amendments, including those addressing greater transparency, requirements for clear and informed consent, notification of profiling and automated processing, privacy assessments for new electronic processing projects, rights to de-indexing (i.e. the right to be forgotten) and data mobility, and a right to present objections to automated processing, will come into force in September 2023.

Quebec's amended law is significant because it represents the only Canadian legislative iteration, either in force or soon to be in force, of what may be characterized as a "second generation" privacy law, of which the EU's GDPR is the most prominent example.

Federal political parties appeal the BC Commissioner's privacy ruling

At the end of March three federal political parties (Liberals, Conservatives, NDP) filed notice of judicial review of a ruling handed down by David Loukidelis, delegate for BC Information and Privacy Commissioner Michael McEvoy, determining that the parties are subject to the province's *Personal Information Protection Act* (BC PIPA).

In his March 1 Order, Mr. Loukidelis, a former commissioner, ruled that the Commissioner has jurisdiction over the activities of the federal political parties (FPPs) in that province, and that such jurisdiction is not ousted by any existing

[3] See, for example, *A Few Questions about Canada's Artificial Intelligence and Data Act*, Centre for International Governance Innovation, August 11, 2022.

[4] *Act respecting the protection of personal information in the private sector*.

federal law, such as PIPEDA or the *Canada Elections Act* (CEA), or by the constitution.[5] The ruling will require the FPPs to comply with PIPA in respect of all of their collection, uses and disclosures of personal information of BC voters and, arguably, compel the parties to provide equivalent protections to voters across Canada.

The FPPs had argued that BC PIPA does not, or cannot, apply to them, citing variously, the potential application of PIPEDA, a necessary limiting of scope of PIPA within the federal context, the existing application of the CEA, and several grounds of non-constitutionality.

Currently, the federal private sector privacy law, PIPEDA, does not expressly apply to the parties, which are subject to certain, limited, privacy rules under the CEA.[6] Two provincial privacy laws do expressly address such application. Alberta PIPA excludes application to political parties. The Québec *Election Act,* with the Law 25 amendments, now expressly extends certain provisions of that province's *Private Sector Law* to the collection of the voters' personal information by provincial parties.[7]

A decision respecting the judicial review application is not expected before late 2023 at the earliest. However it is likely that, whatever the result, it will be appealed to the Supreme Court of Canada. Determination of the issue of provincial law application to the FPPs will be a significant factor in the future course of privacy oversight of political parties at the federal level where, logically, it should be rooted.

New federal Privacy Commissioner

Daniel Therrien's term as federal Commissioner ended on May 31 and, with a brief hiatus, the appointment of his successor, Philippe Dufresne, was confirmed on June 23.

Commissioner Dufresne's background as a constitutional and human rights lawyer for the government will be particularly apt for the role he will play in enforcing the new federal law, once adopted. Mr. Dufresne's previous roles included senior general counsel at the Canadian Human Rights Commission and Law Clerk and Parliamentary Counsel of the House of Commons, responsible for privacy and the protection of the rights and privileges of parliamentarians.

In his confirmation hearings and in a recent speech to the Canadian Bar Association,[8] the new Commissioner identified "three pillars" of his vision of privacy, specifically, privacy as a fundamental right, privacy in support of the public interest and Canada's innovation and competitiveness, and privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens.

Ontario's employee surveillance law

Effective October 11, Ontario's *Working for Workers Act, 2022* amending the *Employment Standards Act, 2000* by requiring employers to implement written policies regarding electronic monitoring, came into force. All employers with 25 or more employees must have a written policy disclosing whether and how they electronically monitor their employees; specifically, employers who meet the threshold on January 1 of each year must have a policy in place before

[5] Order P22-02, *Conservative Party of Canada, Green Party of Canada, Liberal Party of Canada, New Democratic Party of Canada*.
[6] Section 385, *Application for Registration (*of a political party).
[7] Sections 127.22-127.24 (Title III.1 *Protection of the personal information of electors),* in force September 22, 2023.
[8] A vision for privacy: Rights, trust and public interest, Keynote address at CBA Privacy and Access Law Section Online Symposium, November 4, 2022.

March 1 of that year.

Policies must state whether the employer monitors employees electronically, and if so, a description of how and in what circumstances the employer may do so, the purposes for which information obtained may be used, and the date or dates on which the policy is effective or any changes were made to the policy.

Coming out of the pandemic, as employees continue to work from offsite locations, employers are seeking new ways of supervising and measuring their employees' performance remotely. In this context, the new requirements are helpful in requiring employers to tell their employees if, how, and in what circumstances they are being monitored electronically. However the amendments, while serving as a transparency tool, do not provide any substantive protections for employees against privacy-invasive technologies or stipulate what may or may not be appropriate employee surveillance.

The Ontario Information and Privacy Commissioner has noted that from a privacy perspective, the proposed legislation does not go far enough.[9] In her view, workplace surveillance methods should be used only for fair and appropriate purposes and only to the extent they are reasonably necessary to manage the employer-employee relationship. Commissioner Kosseim makes reference to the Alberta and BC PIPAs which stipulate such limitations.

Mobile data – Tim Hortons App

Two significant reports issued in 2022 provide insights into the related issues of data collected from mobile phones, specifically location data, and the definitions and uses of de-identified data.

In its June 1 Report of the *Joint Investigation into location tracking by the Tim Hortons App* the federal Office of the Privacy Commissioner, together with the Commissioners in Quebec, Alberta and BC, provided their findings respecting the extensive collection of customers' mobile phone location data by the Tim Hortons restaurant chain. The data was collected through the app, downloaded by customers onto their phones with the stated purposes of letting them know about nearby locations that they might want to patronize and about special marketing offers available at those locations.

However far beyond simply advising potential customers of nearby restaurant locations only when they opened it, the app in fact was collecting the user's location data constantly, whether or not it was open. The result was that the app provided Tim Hortons with a data feed of the daily travels of its mobile phone user customers, including at their places of work and residence.

The Commissioners' Report provides several important insights into the privacy compliance implications of collection of mobile phone location data, focusing on two compliance issues under PIPEDA and the parallel provincial privacy laws. Firstly, was such collection appropriate, legitimate and reasonable – and therefore permissible – under such laws? Secondly, if it was permissible, was it collected with valid consent? They determined that the "always on" data collection did not meet the test of permissibility and there was no valid consent for such collection.

[9] Bill 88 needs to go further to protect the privacy rights of workers, April 8, 2022.

The Commissioners also made clear that even though the location data did not identify individuals directly (readings were linked only to the user's "device ID") and were only used on an aggregated basis for analysis purposes, de-identified and aggregated data can still constitute personal information. They pointed to case law to the effect that information will be considered personal "where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information".

Mobile data and de-identified information - Public Health Agency of Canada – ETHI Committee Report

Mobile data collection was also the focus of a Report by the parliamentary Committee on Access to Information, Privacy and Ethics (ETHI) regarding the use of de-identified phone data by the Public Health Agency of Canada (PHAC) for purposes of monitoring population movements during the pandemic.

In addition to the specific data collection by PHAC, the Committee examined issues related to the use of de-identified data and big data and the modernization of federal privacy laws. It also looked at the impact of surveillance and the importance of transparency in government institutions to ensure public trust.

PHAC had used anonymized, de-identified, and aggregated mobility location data provided by Telus Communications through its Data for Good program. It was determined that the information did not constitute personal information and that its use did not contravene the *Privacy Act,* the privacy law that applies to PHAC.

The Committee considered the issue of consent, notwithstanding that the relevant data was de-identified and aggregated. It heard evidence regarding procedures for de-identifying data and concerns that even such data could be re-identified. It recommended that individuals should be provided with greater transparency and a clear opportunity to opt out regarding mobility location data collection and use.

While the Committee's Report is instructive of issues relating to potential issues in mobility location data, the evidence it heard left open clarification of the differential characteristics of distinct categories of non-personal information and in particular criteria addressing whether or under what circumstances data can be re-identified and therefore subject to privacy laws. However, the Committee recommended that federal privacy legislation be amended to apply to de-identified and aggregated data and adopt standards for de-identification of data.

Addressing many of the questions left open by the Committee's Report is the proposed revised treatment of de-identified information and anonymized information under Bill C-27. The Bill defines *de-identified information* as information that has been modified so that an individual cannot be directly identified from it, recognizing that a risk of re-identification remains. It defines *anonymized information* as information that has been irreversibly and permanently modified, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information. Bill C-27's proposed approach substantially aligns with treatment of non-personal information under the EU's GDPR and Quebec's Law 25.

Ontario Court of Appeal decision: Failing to prevent a cyber-attack/third party data breach is not intrusion upon seclusion

In a significant decision of the Ontario Court of Appeal released at the end of November, the scope of privacy class actions for cyber-attacks and third party "hacks", based on the tort of intrusion by seclusion, has been severely limited. In *Owsianik v. Equifax Canada* and two cases involving similar facts, heard together,[10] the plaintiffs alleged that their

[10] Obodo v. Trans Union of Canada, Inc., 2021 ONSC 7297 and Winder v. Marriott International, Inc., 2022 ONSC 390.

personal information was compromised when the defendant was affected by a cyber-attack, and that the defendant's cybersecurity measures were inadequate to the point of constituting "reckless" conduct.

The distinguishing aspect of these cases was that the defendants were not alleged to have invaded the class members' privacy, but that they failed to prevent others from doing so.

Claims brought under the tort of intrusion upon seclusion, first recognized in the Court's *Jones v. Tsige* decision, are required to show that: the defendant's conduct was intentional or reckless; the defendant invaded, without lawful justification, the plaintiff's private affairs or concerns; and a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

The Court concluded that the claim for intrusion upon seclusion could not succeed and therefore the proposed class actions should not proceed because it was the hacker's arguably illegal conduct, not any failure to protect the relevant information by the defendants, which constituted the "intrusion". The defendants' recklessness with respect to other conduct, such as care in the storage of the information, does not satisfy the conduct requirement of the tort.

Further, the Court concluded that extending liability for the commission of the intentional tort of invasion of privacy by a stranger to the defendant would not amount to an incremental change in the law. The extension of the common law proposed by the plaintiffs would not be a small step along a well-established path, but would be "a giant step in a very different direction".

Addressing the facts in the *Owsianik* case, the Court stated:

> On the alleged facts, Equifax did not unlawfully access any information. No one acting on Equifax's behalf, or in consort with Equifax, did so. No one for whom Equifax could be held vicariously liable accessed any private information. A third-party stranger to Equifax accessed the information.
>
> To impose liability on Equifax for the tortious conduct of the unknown hackers, as opposed to imposing liability on Equifax for its failure to prevent the hackers from accessing the information, would …. create a new and potentially very broad basis for a finding of liability for intentional torts. A defendant could be liable for any intentional tort committed by anyone, if the defendant owed a duty, under contract, tort, or perhaps under statute, to the plaintiff to protect the plaintiff from the conduct amounting to the intentional tort. (para. 64 and 65)

In sum, the Court stated that the inability to sue the actual hackers is not justification for creating a remedy against a different defendant who has committed a different tort for which the plaintiffs have all the usual remedies available to them; the inability to successfully sue the hacker is no reason to make a defendant liable, not only for its own wrongdoing, but also for the invasion of privacy perpetrated by the hacker.

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