David Young Law
Compliance Bulletin

December 2024

Privacy 2024 Recap – some significant decisions, slow progress for reform

The past year saw a few court decisions of note as well as halting progress toward privacy reform. Other areas of focus included children's privacy and online harms as well as regulation of artificial intelligence. On the reform front, legislation to modernize the federal private sector privacy law, PIPEDA,[1] is stalled in committee and likely will not be passed before the next election. Similarly, the federal initiative to regulate AI - the proposed *Artificial Intelligence and Data Act* (AIDA) – currently linked to the privacy reform under Bill C-27 – likely will not be adopted within that timeframe. However privacy reform and AI regulation are seeing some traction at the provincial level.

OPC v. Facebook – Federal Court of Appeal reverses trial court's decision

In a decision released September 9, 2024[2] the Federal Court of Appeal overturned the Federal Court's trial ruling[3] denying the Privacy Commissioner of Canada's application to order Facebook (now Meta) to rectify the privacy practices that led to the Cambridge Analytica scandal. The trial court had dismissed the application, finding that the Commissioner had not shown that Facebook failed to obtain meaningful consent from users for disclosure of their data to Cambridge Analytica, including for purposes of political targeting, nor had Facebook failed to adequately safeguard user data.

The Court of Appeal ruled that the trial judge erred in his analysis of the relevant provisions of the federal privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), specifically, the provisions addressing meaningful consent and safeguarding data. The most significant aspect of the Court of Appeal's ruling is that determining whether there was meaningful consent must be based on the *standard of a reasonable person*, not the subjective evidence of individual app users.

The trial Court had found that the Commissioner failed to adduce sufficient evidence supporting his determination that Facebook had not obtained meaningful consent and, in particular, any subjective evidence of users regarding their privacy expectations. Furthermore, the Commissioner had not provided any expert evidence as to what Facebook could have done differently. The Court of Appeal disagreed, stating that it was the responsibility of the Court to define an objective, reasonable expectation of meaningful consent.

The Commissioner also found that Facebook did not provide for adequate safeguards to effectively protect users' information in the hands of the apps to which it was disclosed and furthermore was not accountable for users' information that was under its control. Facebook argued that once a user authorizes Facebook to disclose information to an app, its safeguarding duties are at an end. The Court of Appeal again disagreed. Facebook had breached its

[1] *Personal Information Protection and Electronic Documents Act*
[2] Canada (Privacy Commissioner) v. Facebook, Inc., 2024 FCA 140.
[3] Privacy Commissioner of Canada v. Facebook, Inc., 2023 FC 533.

safeguarding obligations during the relevant period by failing to adequately monitor and enforce the contractual compliance and privacy practices of apps operating on its platform.

Privacy compliance by political parties - BC court confirms that PIPA applies to the federal parties

In a decision handed down May 14, the BC Supreme Court ruled that the findings of the provincial Information and Privacy Commissioner's delegated adjudicator, former Commissioner David Loukidelis, confirming application of the province's *Personal Information Protection Act* (PIPA) to federal political parties, were correct. Those findings determined that PIPA applies in full measure to the FPPs, without exception.

The ruling has significance beyond the confines of the province. PIPA's privacy compliance framework is equivalent to that of PIPEDA, which, to date has not been extended expressly to the FPPs. The FPPs had sought to quash the former Commissioner's findings, in part by arguing that the privacy regime applicable to them under the *Canada Elections Act* (CEA) was not only sufficient but that it conflicted with and therefore pre-empted any application of PIPA to the FPPs.

The Court's decision, if not reversed in an appeal,[4] means that, while the FPPs will be subject to PIPEDA-like rules *within BC,* the practical effect will be that they will adopt PIPEDA-compliant procedures *in all provinces and territories*, except to the extent that any local jurisdiction's law applies and differs from PIPEDA. The FPPs will follow this course because they will not want to be perceived as providing privacy rights in one part of the country that are more extensive than elsewhere.

Subsequent to the adjudicator's ruling, the federal government introduced amendments to the CEA which sought to respond to the determination that it does not create a comprehensive privacy regime. Specifically, the amendments (adopted in June 2023) expressly provided that the FPPs may collect, use, disclose, retain and dispose of personal information in accordance with their privacy policies, and that the purpose of the CEA regime was "to provide for a national, uniform, exclusive and complete regime applicable to registered parties and eligible parties respecting their collection, use, disclosure, retention and disposal of personal information".

In testimony before the parliamentary committee that considered these amendments,[5] both the Chief Electoral Officer and the federal Privacy Commissioner stated that the added provisions were inadequate to establish a comprehensive privacy regime, including by pointing to the lack of minimum standards and substantive rights and the limited oversight/enforcement that would be provided by the Chief Electoral Officer. Sensing that the 2023 amendments would be inadequate to establish the constitutional exclusivity of the CEA, the government has tried again to tweak the legislation with a further amending bill, introduced in March 2024,[6] that expands the provisions of the 2023 amendments addressing what should be included in a party's privacy policy and adds a more express oversight power in the Chief Electoral Officer to oversee and scrutinize the parties' policies.

[4] The FPPs have appealed the decision to the BC Court of Appeal, following which a further appeal could be sought before the Supreme Court of Canada.
[5] Senate Standing Committee on Legal and Constitutional Affairs.
[6] Bill C-65.

Privilege in cybersecurity incident investigations – LifeLabs' claim dismissed

Privilege is always an issue in connection with incident investigations involving legal advice.

In responding to a breach incident, the affected party, usually assisted by its legal counsel, may retain cybersecurity consultants to determine the causes of the breach as well as to advise regarding the organization's response and recovery from the incident. The information provided to these consultants likely will include the organization's state of cybersecurity readiness as well as its own analysis regarding the causes of the breach. Because some of this information may indicate deficiencies within the organization's systems leaving it open to allegations of non-compliance with laws and expected standards of privacy and security, potentially leading to financial liability, the organization and its counsel may seek to protect such information from disclosure by way of solicitor-client or litigation privilege.

The Ontario Divisional Court's decision in regards to the Ontario and BC privacy commissioners' investigation into the 2019 LifeLabs security breach provides useful guidance regarding the limited scope for protecting investigation information by way of privilege.[7]

In connection with their investigation, the Commissioners requested to see LifeLabs' consultants' reports. LifeLabs provided the reports but, claiming solicitor-client and litigation privilege, sought to prevent them from publication. The Commissioners denied the claim for privilege. The Ontario Court of Appeal now has refused LifeLabs leave to appeal the Divisional Court's decision, with the result that the Commissioners have released their Investigation Report.

The documents over which LifeLabs asserted solicitor-client or litigation privilege included: the investigation report prepared by its cybersecurity firm which described how the cyberattack occurred; an internal data analysis prepared by LifeLabs describing which health information and which individuals had been affected by the breach; email correspondence between the cyber intelligence firm and the cyber-attackers; and responses by LifeLabs to the Commissioners' specific questions, communicated through legal counsel. With the exception of LifeLabs' internal report, all of the reports and documents were prepared at the request of and provided to their legal counsel.

The Commissioners concluded that, with one exception,[8] their Investigation Report contained facts which existed independently outside the disputed documents that were known to LifeLabs and were required to be provided to the Commissioners pursuant to their joint investigation.

The Commissioners found that none of these disputed documents were subject to solicitor-client or litigation privilege and denied LifeLabs' claims. Importantly, the Commissioners found that facts could not be held back from them simply by virtue of being placed in reports over which privilege was claimed.

In sum, the Court's decision confirms that facts relating to an incident which exist independently outside of any investigation, or which are required by law to be provided to a regulator, cannot be protected by privilege simply by being included within a document, such as a communication with counsel, even if they were compiled by a lawyer.

[7] *LifeLabs LP v. Information and Privacy Commr. (Ontario),* 2024 ONSC 2194 (CanLII); leave to appeal dismissed, November 25, 2024.
[8] The one exception was the written record of the statements made by the cyber-attackers in their correspondence with the cyber intelligence firm that negotiated the payment of the ransom to them. The Court determined that these statements are not subject to solicitor-client privilege.

Privacy reform – Bill C-27

The most significant (and potentially impactful) reform now in place in Canada is found within Quebec's revised Private Privacy Sector Law, Law 25 – arguably the new "bright line" for privacy. While likely several years away from coming into force elsewhere in Canada, the currently stalled initiative to amend the federal private sector law, the proposed *Consumer Privacy Protection Act* CPPA), part of Bill C-27, contains many of the precepts found in the Quebec law and should be used as the relevant point of reference for organizations' privacy compliance programs going forward.

With the minority Parliament now risking an election at any time, it is not clear whether the Bill C-27 instance of federal privacy reform will come to fruition. However it is likely that the major outlines of the proposed CPPA, including the amendments that have been adopted by the INDU Committee[9] – for the most part with all-party support – will find their way into an amended federal law.

The most impactful amendment made to the Bill in committee to date is the recognition of privacy as a fundamental right – sometimes stated as a "fundamental human right". The Bill as originally tabled did not include this precept. Minister Champagne proposed certain amendments to this effect within the preamble to the Bill. However, numerous expert and other stakeholder witnesses advocated for a clearer statement directly addressing the CPPA with the result that all of the recitals to the Bill (minus a recital specific the proposed *Artificial Intelligence and Data Act*) are now included as the preamble to the CPPA, as opposed to the Bill.

A further significant amendment to Bill C-27 made by the Committee is a recognition that the processing of children's information should respect their privacy and best interests. The best interests of the child is the guiding stipulation in the "gold standard" for age-appropriate rules in design of online communications with minors – the UK's *Children's Code*.[10]

Related to its consideration of children's privacy, the Committee adopted an amendment defining the term "minor" - to mean an individual under the age of 18. This age definition will impact the provisions of the CPPA that stipulate special protections for children and other minors, such as the requirement to recognize their best interests in any processing of their personal information, as noted above, and the stipulation that the personal information of minors be considered sensitive information.

Alberta privacy and access law reform

In November, Alberta introduced legislation to bring its public sector privacy law more in line with modern, second-generation privacy laws such as the GDPR[11] and Quebec's Law 25. The proposed new reformed law, the *Protection of Privacy Act* (POPA)[12], provides insight as to what may be expected in updating the province's private sector privacy law,

[9] Standing Committee on Industry and Technology

[10] Age appropriate design: a code of practice for online services, ICO, 2021.

[11] *General Data Protection Regulation*

[12] Bill 33. The province is proposing to divide the existing public sector privacy and access law, the *Freedom of Information and Protection of Privacy Act,* into two separate laws: POPA and the *Access to Information Act* (Bill 34).

the *Personal Information Protection Act*, which currently is undergoing review by a legislative committee, expected to be completed by June 2025.

The new Act will require public organizations to apply the principle of "privacy by design" in developing programs and providing services, put in place comprehensive privacy management programs documenting their privacy practices and promoting compliance with the law, and conduct privacy impact assessments for new programs and systems in circumstances prescribed by regulations. The new Act also will mandate breach notification, an existing requirement under PIPA but to date not provided for under the public sector law.

A significant aspect of the new law is its proposed extension of the public sector law to "non-personal data", which is defined to mean data that has been generated, modified or anonymized so that it does not identify any individual, and is described to encompass de-identified data, anonymized data; and "synthetic data". Along the lines of Quebec's Law 25 regime regarding anonymized data, POPA provides that non-personal data cannot be used to identify or re-identify an individual and must be created using generally accepted best practices in accordance with requirements set out in regulations.

Consistent with evolving requirements for transparency in relation to artificial intelligence in second-generation privacy laws and initiatives to regulate the AI space, governed entities will be required to notify individuals if their personal information is intended to be used in an automated system to generate content or make decisions, recommendations, or predictions.

Oversight of Artificial Intelligence (AI)

The federal government's initiative to regulate certain AI systems under its proposed law, the AIDA, currently stalled in Parliament, is only one of several regulatory and policy developments over the past year in the AI sphere. Additionally, key principles of transparency and explainability are being incorporated into privacy reform initiatives which are going forward even in the absence of AI-specific legislation.[13]

Ontario's *Strengthening Cyber Security and Building Trust in the Public Sector Act*, was adopted in November. Under the new *Enhancing Digital Security Act,* public entities will be required to comply with obligations of transparency and accountability respecting their use of AI, specifically: an obligation to inform the public about its use; an obligation to develop and implement an accountability framework; an obligation to manage risk; and an obligation to provide human oversight.

However, the circumstances under which such obligations will apply and the specific requirements for compliance remain to be set out in regulations. Leaving the key details of regulatory oversight – a criticism of the federal government's approach to regulation under the AIDA – is the subject of a recent blog post by Ontario's Information and Privacy Commissioner: [14]

> Bill 194 regulates some of the most significant digital issues of our time: cybersecurity, artificial intelligence, and children's digital information. Yet it leaves all the critical rulemaking for future regulations to be set by government overseeing its own public institutions. ….. When AI systems influence decisions that touch people's lives, we must demand that they respect the fundamental principles we all value as a society. …. These globally

[13] See, for example, Quebec's Law 25, Alberta's Bill 33 and federal Bill C-27.
[14] "Bill 194: Ontario's missed opportunity to lead on AI"; Dec. 2, 2024.

> recognized principles should [be] codified in Bill 194 to signal a clear government commitment to stand and live by them.

In Quebec, in the absence of specific AI-focussed legislation, the Minister of Cybersecurity and Digital Technology has published, pursuant the *Act respecting the governance and management of information resources of public bodies and government enterprises*,[15] a *Statement of Principles for the Responsible Use of Artificial Intelligence by Public Bodies.* The *Principles* include respect for individual rights, fairness, transparency and accountability, and security.

Youth privacy and online harms

As noted, the federal government's privacy reform, Bill C-27, now includes in the preamble to the CPPA a clear statement to the effect that the processing of children's personal information must address their best interests.

Legislation to protect youth's exposure to harmful content online is gaining traction worldwide. The UK's *Age Appropriate Design Code* has formed the basis of evolving laws and guidance addressing communicating with children online in both Canada and the US.[16] Recently, Australia has banned all social media use by youth under 16.[17]

In Canada, the federal government's *Online Harms Act* (Bill C-63), which received second reading in September, is primarily directed to online bullying, hate speech and non-consented communication of intimate images and more generally "online harm" affecting all individuals. However it includes, significantly, a provision which will require social media platforms to have design features addressing the protection of children. The requirements for such protective features will be set out in regulations, understood potentially to include an age-appropriate design code for youth along the lines of the UK Code.

The provisions of Bill C-63, addressing hate speech had been criticized by civil society advocates as an unconstitutional restriction on freedom of expression. Advocates argued that these provisions need more debate and should be split off from the Bill. However, there was general agreement that the online harms and youth protection provisions of the Bill are desirable and should proceed. The government now has announced that it will adopt this approach with the result that it can be expected that the youth protective provisions, including potentially adoption of an age-appropriate code, may proceed expeditiously through Parliament.[18]

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

[15] CQLR, c. G-1.03
[16] *Youth Forum Report*, BC OIPC, April 2023; California Age-Appropriate Design Code Act.
[17] *Australia Has Barred Everyone Under 16 From Social Media. Will It Work?* New York Times, Nov. 28, 2024.
[18] "Online harms bill to be split between child protections, hate speech: Virani", Global News, Dec. 5, 2024.