David Young Law
Compliance Bulletin

December 2025

2025 Privacy Recap – Youth privacy, breach guidance and other developments

Several significant regulator rulings dominated privacy developments over the past year – focussing on youth privacy and breach response. However, the year also saw important issues of lawful access, freedom of speech and digital sovereignty come into play. On the reform front, a revised federal bill containing selected adjustments to the government's proposed *Consumer Privacy Protection Act* (CPPA) was expected to be introduced before Christmas however the timing now will be (early?) in 2026. Finally, a number of on-going cases progressed, in several instances to appeal.

TikTok Investigation Report – youth privacy and online tracking

In September, the OPC and the privacy regulators in three provinces (Quebec, BC and Alberta) issued the Report of their joint investigation into the personal information collection practices of TikTok, the social media platform particularly popular with youth.[1] The Regulators' investigation focused on issues related to the collection and use of information of children and youth, in particular, the age group 13 to 17, for purposes of ad targeting and content personalization.

The objectives of the investigation were to determine whether the collection, use and disclosure of such information was a permitted, appropriate purpose under the relevant privacy laws and to determine whether TikTok obtained valid consent for purposes of tracking, profiling, targeting and content personalization, including whether it met its obligations to inform users with respect to such uses.

While focussing on the collection and use of personal information of children and youth, the Report contains numerous items of more general compliance guidance. The Report addresses requirements for valid consent on web interfaces, the standard form of privacy policy currently in common usage, consent for biometric information, and consent requirements for profiling and ad targeting.

The TikTok Report also is significant because it contains the first rulings by Quebec's privacy regulator, the Commission d'accès à l'information (the "CAI"), regarding key new provisions of Law 25, that province's reformed *Private Sector Privacy Act,* including those regarding transparency, consent for online data collection, and privacy by default. The CAI's determinations are important because they impact organizations operating in all jurisdictions across Canada.

[1] Joint investigation of TikTok Pte. Ltd. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia and the Office of the Information and Privacy Commissioner of Alberta, PIPEDA Findings # 2025-003, Sept. 23, 2025.

PowerSchool ransomware attack – outsourcing guidance in breach incidents

In December 2024 the education service provider PowerSchool Canada suffered a major data breach across its systems. PowerSchool is an educational technology service provider of student information systems (SIS) to school boards and government education ministries across Canada. The systems are designed to provide data management services related to registration, attendance tracking, scheduling, provincial compliance reporting, staff data management, and management of emergency, medical and health information.

Since the personal information subject of the breach was held by PowerSchool as service provider on behalf of public sector institutions (the school boards and the government ministries), the incident was investigated under the public-sector privacy laws – specifically in two provinces, Ontario and Alberta.[2] The relevant laws stipulate privacy compliance requirements for public sector organizations, which extend to service providers to whom institutions may outsource certain data processing functions , including data storage. However, while the responsibility for compliance lies with the institutions, because the incident involved intrusion into PowerSchool's systems, the investigation of the incident focussed to a large degree on the security protocols of PowerSchool (a private sector organization) as well as the institutions' responsibilities for ensuring that those protocols met the compliance requirements of the public sector laws.

A third party had gained access to PowerSchool's student information system and customer support portal, by using compromised credentials, and obtained personal data held in the SIS including the personal information of current and former students, their parents or guardians, and current and former staff. The cyberattack was discovered when PowerSchool received a ransom demand from the third party.

The investigation reports issued by the Ontario and Alberta regulators are significant because they focus on the obligations of public sector institutions when data processing is outsourced to a service provider. Neither province's public sector laws contain specific provisions regarding outsourcing and in both instances the regulators' conclusions in relation to security protocols were based on the institutions' statutory obligation to protect information by reasonable security measures.[3]

The investigation reports are instructive in providing, in some detail, guidance regarding the regulators' expectations of the institutions for reasonable security measures generally and, more specifically, in circumstances where the institution has outsourced its data processing functions. The guidance provided in the reports includes requirements for contracting with service providers, due diligence obligations with respect to oversight of service providers' security protocols, and minimum standards for breach response policies and protocols.

While the guidance provided in the reports is focussed on compliance requirements for public sector bodies, it can be surmised that it will apply with equal relevance to private sector organizations. In this regard, it is significant that the reports address in some detail the operations of PowerSchool, the private sector service provider, an analysis which of

[2] Ontario: *Freedom of Information and Protection of Privacy Act*, *Municipal Freedom of Information and Protection of Privacy Act*; Alberta: *Freedom of Information and Protection of Privacy Act*.
[3] Ontario FIPPA, Reg. s. 4 (1); MFIPPA Reg. s. 3(1); Alberta FIPPA s. 38.

course would have equal application in circumstances where the service provider is contracting with a private sector organization.

Clearview AI – Alberta PIPA offends the Charter's freedom of speech protection

In a decision released in May, an Alberta court struck down as unconstitutional the exception provisions of Alberta PIPA providing for the collection, use and disclosure of personal information without consent on the basis that it is "publicly available".[4] As under the federal privacy law, PIPEDA,[5] Alberta PIPA's exception to the consent requirement provides for information made available publicly through stipulated forms of media, including magazines, books and newspapers. Clearview AI, the facial recognition tool provider, as part of its operations conducted scraping the internet for images of individuals for purposes of adding to its database of billions of images and information for purposes of matching facial images for clients. In connection with a joint investigation into these activities by the BC, Alberta, Quebec and federal privacy regulators,[6] Clearview had argued that it was permitted to collect facial recognition data from social media and other internet websites on the basis that such platforms fell under the publicly available exception. The Alberta OIPC issued an order requiring Clearview to cease such scraping on the basis that its collection, use and disclosure of the information was not a reasonable purpose, which Clearview challenged in court.

While the Alberta court agreed with the Commissioner's determination that the non-exhaustive categories of media prescribed by regulation as eligible for the exception (magazines, books, newspapers) do not extend to online media sources such as websites and social media platforms, it agreed with Clearview's assertion that limiting the publicly available exception to such categories constitutes a breach of the Charter's right to freedom of speech and expression in the *Canadian Charter of Rights and Freedoms*. As a result, the court ruled the provisions unconstitutional.

Clearview had argued that its scraping activity is expressive because it facilitates the provision of its facial recognition services (*i.e.* information) to customers. The Court concluded that personal information including images collected by Clearview is integrally related to the development of "thought, belief, opinion and expression", which is protected by section 2(b) of the Charter – the right to freedom of expression. The Court analogized Clearview's scraping to search engines which collect data for purposes of indexing and providing search results for internet users, arguing that such activities should be protected by the Charter right. Further, there was no justification for imposing a blanket consent requirement for the collection, use and disclosure of personal information publicly available on the internet without privacy settings.

Although the Court acknowledged that Alberta likely has a legitimate interest in protecting personal information from being used in a facial recognition database like Clearview's (due to the potential harms to individuals' privacy), the Court concluded that PIPA and the Regulation are overbroad because they restrict other expression for which there is no such justification (*e.g.*, regular search engines).

---

[4] *Personal Information Protection Act, ss 12, 17, 20.*
[5] *Personal Information Protection and Electronic Documents Act*.
[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 Findings #2021-001; Feb. 2, 2021.

The decision has been appealed by Clearview in relation to the Court's findings that PIPA has jurisdiction over Clearview, which it argued did not carry on business in Alberta, and the Commissioner's finding that Clearview did not have a reasonable purpose for collecting, using and disclosing the relevant information. It is not known yet whether the constitutionality issue will be subject of an appeal.

Privacy reform, lawful access and application to political parties – legislative updates

With the federal government's privacy reform Bill C-27 dying in the last Parliament, there has been high expectation of a revised CPPA being tabled before Christmas. However, since Parliament has now adjourned, this will not happen and instead the likely timing will be late January or early February.

The federal government's proposed *Strong Borders Act* (Bill C-2), introduced in June, included provisions that would significantly expand the ability of law enforcement and national security authorities to obtain personal data from any organization in connection with an investigation, without a warrant. As a result of wide criticism of these proposals, the government introduced a new bill (Bill C-12) omitting the warrantless search provisions. However, in recent pronouncements, the government has indicated that these proposed search provisions would be enacted, as originally tabled, and the original version of Bill C-2 continues to progress through Parliament.

Separately, the government is making another attempt to clearly exclude political parties from the application of federal privacy law, with its tacking onto a bill otherwise dealing with taxation and regulated pricing matters, proposed further amendments to the *Canada Elections Act* (CEA) designed to once and for all put out to pasture the determination by the BC Information and Privacy Commissioner to have oversight of the privacy practices of the federal political parties in that province.

It will be remembered that In a 2024 decision the BC Supreme Court confirmed the application of the province's *Personal Information Protection Act* (PIPA) to federal political parties (FPPs). The ruling has significance beyond the province. PIPA's privacy compliance framework is equivalent to that of the federal law, PIPEDA, which, to date has not been extended expressly to the FPPs. The FPPs that brought the judicial review application had sought to quash the BC Information and Privacy Commissioner's determination that PIPA applies to them. The FPPs have appealed the court's ruling. However, the proposed new CEA provisions attempt to pre-empt any reason for an appeal by adding express provisions excluding the FPPs from oversight by a provincial or territorial legislature.

Digital sovereignty – proposals for blocking statutes

In the context of the current trade environment, concerns for digital sovereignty, in particular the integrity of digital systems and data, have resulted in commentaries and initiatives by subject matter experts and others urging action to strengthen protections for Canada's technology infrastructure.[7] These commentaries range from identifying

[7] See, for example: How to Confront Canada's Digital Dependence, Heidi Tworek and Alicia Wanless , CIGI Online, July 1, 2025; Canada is becoming digitally subservient to the US in the global economy, Barry Appleton, The Globe and Mail, July 19 , 2025; Ensuring the sovereignty and security of Canadian health data, Michael Geist, Mari Teitelbaum and Kumanan Wilson, Canadian

requirements for locally-based data cloud and other data storage capabilities, including "data residency" or "localization" requirements, to proposing enhancing privacy protections for Canadians' data transferred outside the country.

Of particular note among these proposals is one for enacting so-called "blocking statutes". Blocking statutes involve the adoption of privacy-protecting laws to counter mandated disclosure of data held by an entity in the local jurisdiction, as a result of an order or law in another jurisdiction that may apply extra-territorially. The local entity would face penalties for disclosure if it responds to the order or law in the foreign jurisdiction. An instance of when such a statute could have application is the 2018 US *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) which authorizes US law enforcement agencies to access data held by US entities in foreign countries.

In the context of these initiatives for digital sovereignty and the discussion of blocking statutes, it is interesting to note the recent case of *R. v. OVH.* In that case, an Ontario court not only ordered disclosure of data held in France by the parent of a Canadian subsidiary but did so in the face of a French "blocking statute" which the court acknowledged had application but characterized it as rarely enforced.[8]

Facebook/Cambridge Analytica

This important case, involving the interpretation of PIPEDA's requirements for valid consent, has been appealed by Facebook/Meta to the Supreme Court of Canada and will be argued there in March. It will be recalled that the case involves whether meaningful consent to collect and disclose the personal information of app users must be based on the standard of a reasonable person, or on the potentially more limited basis of the subjective evidence of individual users.

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

Medical Association Journal, July 28, 2025; Open Letter to Prime Minister Carney, concerned individuals and civil society organizations, September 2, 2025.

[8] Ontario Court of Justice, Sept. 19, 2025. For a commentary on this case, see David Fraser, *Canadian Privacy Blog*, Dec. 5, 2025.