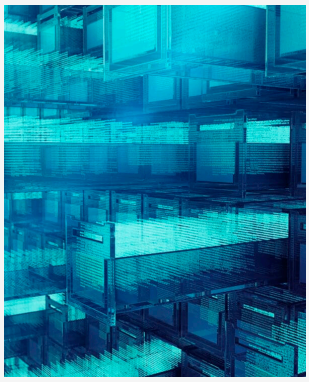
OSLER

10 Privacy Trends of 2025

This is the third in a series of articles recapping the second annual Privacy Conference in Montréal.

DECEMBER 9, 2025 12 MIN READ



Related Expertise

- Artificial Intelligence
- Corporate Governance
- Disputes
- Privacy and Data Management
- Privacy and Data Security Disputes
- Technology

Authors: Éloïse Gratton, Ad. E., François Joli-Coeur

In October, Osler's Montréal office hosted the firm's second annual Privacy Conference organized by its Privacy and Data Management team. The half-day program, followed by a networking lunch, brought together industry experts and in-house counsel to discuss a range of hot topics, including the implementation of amendments introduced by Law 25, emerging litigation trends, artificial intelligence governance, new technologies and cybersecurity.

The conference opened with a review of the year's 10 most significant privacy trends, presented by Éloïse Gratton, partner and Co-Chair of Osler's national Privacy and Data Management practice, and François Joli-Cœur, partner.

We have already posted articles about: Cybersecurity and privacy: key takeaways from our second annual conference and The privacy officer's changing role in the age of innovation and AI. In the coming weeks, we will post articles on the other two major topics discussed at the conference:

- Year-in-review: privacy litigation
- Artificial intelligence: governance and other emerging issues

Below are the key privacy trends from the past year and takeaways for your organization.

1. Biometrics: rapid adoption and increasing risk

The use of biometrics is expanding quickly across all sectors, from workplace access control and timekeeping systems to retail loss prevention and digital identity verification. Canadian privacy regulators remain particularly active in this area.

In 2024–2025, Québec's Commission d'accès à l'information (CAI) received more than 100 biometrics collection notifications[1] under the *Act to establish a legal framework for information technology* — a 206% increase in three years. This growth reflects the rising popularity of biometric authentication and identification methods.

Organizations that notify the CAI of their use of biometrics often receive response letters suggesting potential noncompliance (e.g., invalid consent, failure to meet the

necessity/proportionality test, lack of an alternative measure). These letters are not formal or binding decisions; they identify potential violations based on the CAI's preliminary review of the submitted documentation.

With respect to formal investigations, the CAI reaffirmed its skepticism about the necessity and proportionality of biometric systems in its Métro (2025) and Transcontinental (2024) decisions, issued under the *Act respecting the protection of personal information in the private sector* (ARPPIPS). This approach stems from the CAI's view that biometric data is particularly sensitive due to its unique and immutable nature. Consequently, the CAI requires organizations to provide concrete evidence that the collection serves an important, legitimate and real purpose, and that the privacy impact is proportionate to that purpose.

At the federal level, the Office of the Privacy Commissioner of Canada (OPC) released its Guidance for processing biometrics – for businesses. These new guidelines outline key factors and principles that organizations must consider when designing or deploying biometric initiatives, including

- the need to demonstrate that the purpose of the initiative is legitimate, appropriate and proportionate to the privacy risks
- the requirements for obtaining valid consent
- the importance of data minimization, transparency, robust safeguards and maintaining the accuracy of biometric systems

Unlike the CAI's position, the OPC acknowledges that, in some circumstances, biometrics may be required as a condition of service (i.e., no alternative is offered).

Authorities are also broadening the definition of "biometric data." Following their investigation into the social media platform TikTok, the federal and provincial commissioners classified certain non-identifying traits as biometric. This suggests that any technology capable of analyzing physiological or behavioural characteristics may trigger additional obligations. Organizations using such technologies should reassess whether their practices fall within the scope of biometric processing and adjust their internal governance accordingly.

Key takeaway: Between the CAI's strict interpretation and the OPC's more nuanced framework for biometrics, organizations must determine their position on the risk-and-compliance spectrum while rigourously documenting the necessity and proportionality of their biometric practices.

2. Privacy incidents: new threats and surge in reports

Since Québec's breach-notification requirements took effect in 2022,[2] the CAI has seen a 559% increase in reports, receiving a total of 514 in 2024–2025.[3] At the federal level, the OPC received 615 data breach reports during the same period, a volume similar to the previous year.[4]

The increase in reporting can be partly explained by improved incident detection tools and greater awareness of personal information protection issues within organizations — often encouraged by regulators themselves. However, this heightened transparency is accompanied by closer regulatory scrutiny, creating a dynamic in which meeting expectations around prevention and reporting can paradoxically increase the likelihood of an investigation. Canadian privacy regulators, including the CAI and the OPC, are conducting more post-notification follow-ups to assess whether organizations are taking steps to

prevent similar incidents. For now, however, regulators are focusing their oversight efforts on major incidents.

Attacks are becoming increasingly complex and often target supply chains and critical infrastructure. In June 2025, Bill C-8 was introduced to establish the *Critical Cyber Systems Protection Act*, which provides a framework for the protection of critical cyber systems of services and systems vital to national security or public safety. There has also been an increase in insider attacks, forcing organizations to develop more sophisticated detection systems.

In response to the evolving threat landscape, organizations are conducting tabletop exercises and implementing formal incident response procedures.

Key takeaway: As investigations and regulatory follow-ups triggered by breach notifications become more frequent, organizations should strengthen their prevention practices by reinforcing their physical, organizational and administrative safeguards. Doing so reduces incident risks at the source and helps avoid potential investigations. Heightened vigilance is also needed against insider threats, which are often underestimated.

3. Access requests: from compliance tool to litigation strategy

Access requests under personal information protection laws are increasingly being used as strategic tools to prepare litigation against organizations or to support complaints before regulatory authorities. More and more, these requests are being drafted by generative AI, resulting in a notable increase in numbers and sophistication — and, by extension, their relevance in legal disputes. They now target a much broader range of information and often include extremely detailed descriptions of the data sought, such as metadata, logs, internal scores and other derived data.

As the volume of requests rises, some organizations are turning to automated triage and response processes. However, these systems can fail. For instance, they sometimes generate overly generic responses that fail to meet the specific requirements of applicable laws. When a response is incomplete or delayed, the person may file a complaint with regulatory authorities. Organizations must therefore ensure that responses generated through automated processes are legally defensible. This includes clearly informing users that these tools are not intended to provide full access to all information held by the organization, but rather to facilitate self-service access to certain data, while also explaining how users can obtain additional information. Close collaboration between legal and technical teams is equally important to efficiently extract relevant data and ensure consistent communication.

Key takeaway: As access requests continue to increase in numbers and complexity, organizations must strengthen the maturity and capacity of their access request management programs. Although automated processes can improve efficiency, they must be designed and supervised to remain legally defensible, transparent and compliant with applicable legal requirements.

4. Children's privacy: a national priority

Children's privacy is a growing regulatory and political priority.

On the legislative front, Innovation Minister Evan Solomon has confirmed that protecting young people is a core principle guiding upcoming federal reforms.[5] This aligns with a broader international trend, as several jurisdictions, including the European Union, already

have stricter requirements to protect minors' data.

A joint investigation into the social media platform TikTok also shed light on practices surrounding the collection, use and disclosure of children's personal information. The Office of the Privacy Commissioner of Canada (OPC) now considers children's personal information to be sensitive by default[6] and is conducting a consultation on a Children's Privacy Code. The OPC recently finished a consultation on age assurance. Organizations must navigate differing privacy age-of-consent thresholds across jurisdictions. In Québec, the threshold is 14, while the rest of Canada is aligning around age 13, creating divergent compliance obligations.

This heightened scrutiny brings increased legal risk. In Québec, for example, dozens of video game developers are currently facing a class action lawsuit for alleged violations of children's privacy.

Key takeaway: As children's privacy becomes more prominent in regulatory and policy agendas, companies offering digital services aimed at young users should prepare for greater oversight of age verification mechanisms and more stringent consent validation and transparency requirements.

5. Data sovereignty: political stakes and infrastructure choices

The debate around data localization and foreign access to data is now translating into concrete requirements. In 2025, governments and large enterprises are demanding greater control over the location of Canadian data.

Concerns about the U.S. CLOUD Act are fueling caution around cross-border data hosting. Many organizations now deal only with hosting providers based in Canada, or, when they do deal with foreign providers, they require that their domestic data be subject only to Canadian jurisdictions. At the same time, some public bodies are incorporating localization clauses into their procurement processes.

The Canadian Sovereign AI Compute Strategy demonstrates that digital sovereignty is becoming a cornerstone of industrial policy and AI governance.

For the private sector, this shift requires balancing efficiency with compliance, often through sovereign or hybrid cloud solutions.

Key takeaway: As digital sovereignty becomes a political and contractual issue, organizations should incorporate it into their strategic planning and risk mapping to anticipate growing regulatory and client expectations.

6. Enforcement: more investigations, no fines yet

Despite the expanded powers granted to the CAI through the amendments introduced by Law 25, the CAI has yet to impose any administrative monetary penalties. It is, however, stepping up its investigative activity. Recent decisions involve a broader range of organizations, including Quebec-based retailers and manufacturers. Joint investigations with other Canadian regulators are increasing, and authorities are paying closer attention to insider threats and internal misuse of data.

Key takeaway: The absence of fines should not be interpreted as leniency. Expectations for mature and effective privacy management programs continue to grow.

7. Surveillance technologies: balancing security and compliance

Amid rising security risks, organizations are adopting various monitoring technologies — such as in-store analytics, employee tracking and behavioural detection. The Métro decision highlighted the tension between a company's right to prevent losses and its obligation to respect individuals' privacy: legitimate security objectives must be proportionate and grounded in a rigourous assessment of the need for the measures deployed.

In the workplace, remote monitoring, cameras and productivity tracking raise similar challenges, meaning that transparency, data minimization and clear internal policies are essential.

Online, AI-driven behavioural analytics blur the boundaries between security, profiling and consent. Organizations must document their purposes and assess risks, particularly when automated decisions affect individuals' rights or employment. Privacy impact assessments (PIAs) and the development of an algorithmic governance framework are then essential components of responsible digital surveillance practices.

Key takeaway: Organizations expanding their use of surveillance technologies for security purposes must carefully plan deployment, assess necessity and proportionality, incorporate privacy-by-design principles, and ensure rigourous documentation.

8. Profiling and privacy by default: the next interpretive frontier

In Québec, the new rules on automated decision-making and privacy by default have established a complex implementation framework, especially for AI systems that are continuously evolving. Organizations must revisit their user interfaces, default settings and internal review mechanisms to ensure transparent and fair personalization. They should also be able to explain the logic behind their systems and document the nature of the inferences they generate.

Additional complexities unique to the Québec context emerge in the CAI decision issued under the ARPPIPS and set out in joint investigation report #2025-003. In it, the CAI explains that Québec's privacy-by-default rules differ from those of the EU because the wording in ARPPIPS section 9.1 is different from the wording in GDPR section 25. This distinction adds another layer of uncertainty regarding the practical scope of privacy-by-default obligations and regulators' expectations.

Key takeaway: Profiling and privacy by default are still uncertain areas of law both at the federal level and in Québec, so organizations must proceed with caution. Organizations should closely monitor evolving standards, anticipate grey areas in their personalization practices, and prepare to quickly adapt their systems and processes as regulatory expectations develop.

9. Deceptive design: consent under scrutiny

The OPC opened a new enforcement front with its 2024 report on manipulative design practices. Regulators are now examining not only whether a user consents, but also how that consent is obtained.

"Dark pattern" practices such as pre-checked boxes, misleading wording, repeated prompts and artificial barriers can invalidate consent. The OPC has identified four problematic

categories — interference, obstruction, coercion and harassment — that align with international standards, including those of the EU's *Digital Services Act*.

Key takeaway: As regulators pay closer attention to how consent is obtained, Canadian organizations should reevaluate their interfaces and privacy settings. Consent is becoming as much a matter of design governance as legal compliance.

10. Artificial intelligence: the new stress test for privacy law

AI is reshaping privacy compliance in fundamental ways. Joint investigations into OpenAI and X (formerly Twitter) demonstrate regulators' intensifying concern over user data being recycled for secondary purposes and model training. Even major international companies like these are not immune to rigourous regulatory scrutiny.

Several key questions now dominate the Canadian landscape

- Can organizations use customer or internal data to train AI models without explicit consent?
- How can contracts limit a vendor's ability to use customer data to train its own systems?
- When does the use of AI assistants or scribes trigger the obligation to disclose automated decision-making under section 12.1 of Québec's ARPPIPS?

These questions underscore the growing importance of purpose transparency, explainability and limitation in AI use. By 2026, privacy compliance programs will be inextricably linked to AI governance.

Key takeaway: As regulatory scrutiny over data used for AI training intensifies, organizations must establish integrated processes for managing data and algorithms. Close collaboration among legal, technical and ethics teams is required to ensure responsible AI use and strengthen customer and partner trust.

Conclusion: a year defined by accountability

These 10 trends have one thing in common: regulators now expect organizations to demonstrate true accountability by documenting the necessity of their initiatives, explaining their choices and embedding personal information protection into their day-to-day operations, rather than simply complying with the law.

The intersection of privacy, cybersecurity and artificial intelligence is tightening rapidly. In the coming months, Osler's AccessPrivacy team will publish follow-up analyses on several conference themes, including AI governance, children's privacy and emerging class-action risks.

For privacy professionals, 2025 has been both a year of adaptation and the start of a new era of integrated, risk-based governance in Canada.

---

[1] CAI, Rapport annuel d'activités et de gestion 2024–2025) (in French).

[2] ARPPIPS, section 3.5.

[3] CAI, Rapport annuel d'activités et de gestion 2024-2025 (October 2025, in French)

[4] OPC, "2024–2025 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*" (June 5, 2025)

[5] Toronto Star, "Evan Solomon says lessons from TikTok privacy probe will help shape new Canadian AI laws" (September 24, 2025)

[6] Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight, Putting best interests of young people at the forefront of privacy and access to personal information – Office of the Privacy Commissioner of Canada (October 4–5, 2023)