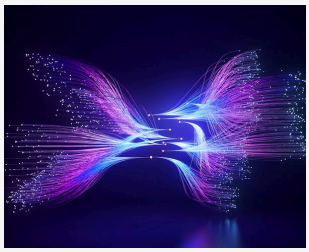
OSLER

Year-in-review: privacy litigation highlights



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

Access all five Updates in this series

FEBRUARY 2, 2026 4 MIN READ

Related Expertise

- Artificial Intelligence
- Corporate Governance
- Disputes
- Intellectual Property
- Privacy and Data Management
- Risk Management and Crisis Response
- Technology

Authors: Kristian Brabander, Jessica Harding, Julien Morissette, François Joli-Coeur

Key Takeaways

- Osler's Privacy Conference discussed key trends in privacy law, focusing on litigation and regulatory decisions.
- Recent cases highlight the significance of regulatory actions, particularly in biometric data use and personal information disclosure.
- Privacy litigation now represents a strategic area of litigation.

Last fall, 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.

As part of the conference, litigation partners Kristian Brabander, Jessica Harding and Julien Morissette looked back on a particularly active year of privacy-related decisions, investigations and proceedings.

A clear theme emerged: litigation involving personal information is expanding across a wider range of industries and is heavily shaped by regulatory decisions.

What follows are the key takeaways from their presentation.

Regulatory litigation as a leading indicator of emerging risks

According to Julien Morissette, matters brought before regulators — such as Québec's Commission d'accès à l'information (CAI) — often act as a canary in the coal mine**.** Regulators can surface issues that later drive class actions and other major lawsuits. Two recent examples stand out: one involving biometric data, and the other involving personal information about corporate representatives.

In a CAI decision involving Imprimeries Transcontinental Inc., 1024350-S, the CAI's oversight division reiterated that collecting biometric data must be tied to a legitimate, significant and demonstrated objective, and must meet a strict proportionality requirement. Finding that the employer had not shown sufficient security concerns to justify the continued use of a facial recognition system introduced during the pandemic as an access control measure, the CAI ordered the system shut down and its biometric templates destroyed. For a more detailed discussion, see our Update: Québec privacy commissioner continues to set high bar for biometric data processing: lessons for business, on this decision.

In *Centre d'acquisitions gouvernementales c. Teva Canada limitée*, 2025 QCCQ 892, the Court of Québec (hearing an appeal from a CAI decision) confirmed that the names and contact information of individuals acting as representatives of a corporation do not constitute confidential personal information. As a result, a public body must disclose such information in response to an access to information request.

Key summary points

- An access to information request does not automatically fall within an exemption from disclosure
- A document does not need to be expressly contemplated by an organization's mandate to be considered "held" by that body and therefore subject to disclosure
- The name of a corporate representative is not, in itself, confidential personal information

This important decision confirms that, with respect to the names and contact information of individuals acting on behalf of a corporation, the right of access to information prevails. For a more detailed discussion, see our Update: Québec court issues key decision on public access to . . . access to information requests, on this decision.

Cybersecurity-related class actions: steady growth

Jessica Harding noted a sustained increase in class actions following security incidents, reflected in a series of proceedings filed in Québec in 2024–2025 across sectors and industries.

1. The Capital One decision: clarification at the authorization stage

In *Royer c. Capital One Bank*, 2025 QCCA 217, the Court of Appeal adopted a broader approach at the authorization stage, confirming that

- the representative's personal cause of action does not need to reflect that of every class member
- it is not necessary at this stage to determine whether non-pecuniary losses are compensable
- the claim for punitive damages could proceed

This decision reinforces a trend already evident since Lamoureux: the authorization threshold remains low, including for privacy-related class actions.

2. Suncor: alleged fault and consumer-facing representations

In *Harguindeguy c. Suncor*, 2025 QCCS 3072, the Superior Court authorized the class action in part following an incident affecting members of the Petro-Points program.

The Court found, in particular

- an arguable case of contractual fault
- an arguable claim based on misleading representations within the meaning of the *Consumer Protection Act*
- that the requested injunction was overly broad, as it sought a permanent order requiring Suncor to provide class members with credit and fraud monitoring services and anti-tracking equipment

The decision highlights how difficult it can be for businesses to challenge allegations at this preliminary stage.

Trends in class action: broader and cross-border

Kristian Brabander noted two major trends

- actions being filed in Canada following major U.S. settlements
- a surge in privacy- and AI-related claims, including allegations of copyright infringement (for example, web scraping to train AI models) and allegations that tech companies collected personal information without authorization

Conclusion: a more contentious, fast-moving and complex landscape

This annual review confirmed the following: privacy has become a strategic area of litigation. At this intersection of regulatory decisions, security incidents and technology practices, plaintiffs are becoming increasingly creative and regulatory bodies are stepping up their work.