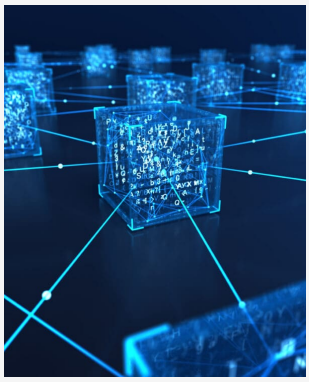
OSLER

The privacy officer's changing role in the age of innovation and AI



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

NOVEMBER 28, 2025 6 MIN READ

Related Expertise

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

Author: Éloïse Gratton, Ad. E.

Key takeaways

- The privacy officer's role has evolved from compliance to being a strategic partner in innovation and governance.
- Experts emphasized the need for privacy officers to collaborate closely with departments like IT and cybersecurity.
- Ultimately, data privacy is a competitive advantage, essential for sustaining trust and innovation in organizations.

Last month Osler's Montréal office hosted the firm's second annual Privacy Conference, organized by the 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 (AI) governance, new technologies and cybersecurity.

One high point was a panel moderated by Eloïse Gratton, partner and Co-Chair of Osler's national Privacy and Data Management practice, on emerging privacy risks and the changing role of in-house counsel. Three renowned experts shared their experiences

- Anthony Hémond, Lawyer – Senior Counsel, Privacy, Air Canada
- Jasmine Adhami, Senior Director, Legal Affairs and Privacy Officer, Dollarama
- Selina Sforza, Director, Legal Operations, Alimentation Couche-Tard

Their discussion brought forward a shared conclusion: that today's privacy officer is a strategic player straddling the fields of law, technology and corporate governance.

From compliance to strategy: an evolving role

The panellists emphasized that the privacy officer's role has changed dramatically. Once viewed as a siloed compliance task, data privacy has become a driver of governance and innovation.
Selina sees this shift translating into much closer day-to-day collaboration with innovation

teams. “We work directly with development and innovation teams to build privacy right into the product at the design stage,” she explained. “It’s still compliance, but it’s also — and especially — a tool for responsible innovation.”

This transformation requires more agility in adapting to changing laws. Jasmine pointed out that “it can take months or even years for regulators to catch up with new legislation,” which means organizations have to adjust their strategies in midstream. She sees the privacy officer’s role as being one of adaptation and risk comprehension. “We have to navigate uncertainty while keeping our program coherent.”

Anthony emphasized the technological aspect of data privacy. “The privacy officer has to be an expert in cybersecurity, data governance and, more and more, AI. It’s a hybrid role, dealing in both law and technology.”

These comments point to a radical transformation: the privacy officer is no longer a simple compliance watchdog, but a business partner who helps the organization innovate responsibly.

Making data privacy matter to management

How can we get management to commit fully to data privacy? This core question elicited a rich exchange.

For Jasmine, the key is to “forge direct ties with strategic departments such as projects, innovation and cybersecurity, and be present on risk management and architecture committees.” She also emphasized the importance of staying pragmatic. “Short, targeted messages are much more effective than a long report. For example, an email summarizing a judgment enforceable abroad can spark immediate dialogue and keep privacy issues on management’s agenda.”

In Anthony’s opinion, board members will only become more aware if they are made accountable. “Recent decisions where boards were held liable for cybersecurity incidents have been game changers,” he noted, adding that compliance can even be a competitive advantage. “Some companies in Europe cite their GDPR compliance to show their reliability and to stand out from their less meticulous competitors.”

Selina, who bases her approach on brand value, said that, in her experience, management will pay attention to messages that speak in terms of business risks and opportunities. “Describing the risks and giving concrete examples will often have more impact than expounding on the topic at length,” she explained. “Data privacy is also about sustainability and brand trust.”

Fostering an organizational culture of respect for privacy

The panellists then tackled an often-overlooked question: how do we get beyond mandatory workshops and internal policies to make data privacy an ingrained part of the corporate culture?

Selina sits on an internal AI council comprised of people from Legal, Cybersecurity, Marketing and other key departments. She explained: “Any project involving AI, whether internal or led by a supplier, has to go through the council.” The council members meet weekly to assess risks and ensure coherent decisions.

Jasmine participates in monthly project review meetings attended by people from IT, innovation and data privacy: “Any initiative involving personal information has to be presented at these meetings, along with a brief assessment of its privacy-related aspects.” This fosters accountability without creating red tape. “We want to be partners, not obstructionists,” she pointed out. “Privacy shouldn’t be seen as a hindrance, but as a natural component of innovation.”

Anthony noted that collaboration now extends to processes that traditionally had nothing to do with law: “Our privacy teams are involved in calls for tenders and contract redlining, looking in particular at cross-border data transfers.” In his opinion, a program can only be successful if it harmoniously integrates people with processes and technologies.

All three experts agreed that data privacy management cannot rely solely on policies: it has to be part of daily operations, supported by a clear, collaborative structure and by recognition of its importance at all organizational levels.

AI, biometrics and surveillance: navigating a shifting legal landscape

Lawmakers are struggling to keep up with new issues arising from the emergence of AI, biometric tools and surveillance technologies.

Anthony opened this part of the discussion by observing that “regulatory guidelines often lag behind technology,” leaving organizations in a grey zone, especially regarding the use of generative AI. “We need to take a proactive, responsible approach, even when the legal framework isn’t clear yet,” he added.

To illustrate this point, Jasmine cited a pilot project with the business consulting group at the Office of the Privacy Commissioner of Canada (OPC). “After our project demonstration, a privacy assessment, and constructive exchanges with the OPC, we got recommendations for improving project design and consent.” As she sees it, this experience shows the advantage of collaborating upstream with regulators. “It’s much more productive to involve them early rather than wait for an investigation or sanction.”

The panellists all agreed that, in a technological environment that is moving faster than the law, proactive governance and transparency are of critical importance. An organization that anticipates risks will be in a better position to innovate responsibly.

Advice to in-house counsel: understand the technological context

When asked what organizations should expect from their in-house counsel, all the panellists emphasized the importance of an in-depth knowledge of technology.

Jasmine recommended that lawyers “understand data flows, cloud environments and systems” to provide actionable legal advice. “We can’t keep focusing on laws: we have to know how data actually circulates in the organization,” she argued.

Selina concurred, saying that “a sound legal opinion is based on a firm grasp of the business and the technologies. You have to know what the company is buying, why, and how that fits in with its operations.”

Lastly, Anthony emphasized the value of networking: “In Europe, privacy officers have

associations where they can compare practices and learn from each other, and that's something we should have in Canada as well."

These comments are a reminder that privacy is no longer a concern of privacy officers alone: it requires constant collaboration between lawyers, technicians and managers, with each contributing to overall data governance.

Conclusion: privacy as a cornerstone of trust and competitiveness

As the panel demonstrated, the privacy officer's role has evolved from compliance watchdog to a guardian of digital trust.

In closing, Eloïse remarked that "data privacy is no longer just a regulatory obligation, but a corporate value and a competitive advantage. Organizations that build it into their innovation strategy will come out winners."

As corporate priorities are reshaped by AI, cybersecurity and data governance, the privacy officer's role will continue to evolve away from reacting to laws and toward true leadership in ethical and sustainable innovation.