Artificial intelligence and privacy: highlights from our second annual conference in Montréal

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

Access all five Updates in this series

JANUARY 19, 2026 6 MIN READ

Related Expertise

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

Author: François Joli-Coeur

Key takeaways

- Frédérique Horwood noted the rise of agentic AI, highlighting its autonomy compared to traditional AI.
- Risks of agentic AI include prompt injection and cascading failure, requiring careful rollout and monitoring.
- The governance landscape for AI is evolving, with different responsibilities for developers and users in B2B and B2C contexts.

During the 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 (AI) governance, new technologies, and cybersecurity.

One highlight of the event was a conversation between partner François Joli-Coeur from the national Privacy and Data Management practice, and Frédérique Horwood, Senior Counsel, Privacy and AI Regulation at Cohere. What follows are the key insights from their discussion, along with useful perspectives for Canadian businesses.

Frédérique Horwood: working daily at the intersection of AI and privacy protection

Privacy and agentic AI

On the hot topic of agentic AI, Frédérique began by pointing out that this concept still lacks a universally accepted definition. Still, she offered a helpful distinction that sheds light on the issues raised by agentic AI:

- "Traditional" AI carries out predictable, well-defined and repetitive tasks. This can include auto-populating templates, analyzing a series of documents, or carrying out a sequence of predefined tasks.
- In contrast, agentic AI stands out for its greater autonomy, recall and adaptability. Agentic AI can understand context, draw conclusions, make decisions, proactively initiate a course of action, and fine-tune its behaviour over time. This makes it a more adaptive form of AI that can act as your digital teammate.

Main risks

Agentic AI introduces new types of risk for businesses.[1] The speakers addressed two of its main risks:

- Prompt injection: malicious instructions hidden in agent prompts or embedded in its "memory", or working context, can alter how it behaves.
- Cascading failure: Agentic AI expands a business's attack surface. Since agents typically connect to several systems, failures and malicious attacks can have cascading effects.

While agentic AI offers productivity gains, it also demands careful consideration of how it is rolled out, monitored and integrated into operational processes.

Examples of how corporate legal teams use AI agents

Agent-driven AI tools can help in-house legal departments by automating certain tasks, including

- reviewing contracts and performing due diligence
- sorting and categorizing email
- creating dashboards and reports

Frédérique also surveyed the participants on whether their organizations had begun rolling out AI agents for tasks like conducting privacy impact assessments (PIAs) or reviewing data processing agreements (DPAs). The small number of positive responses led her to observe that, even though these tools are rapidly gaining ground among AI-driven organizations in Canada and the United States, their adoption remains limited in many Canadian business sectors.

AI governance: roles and responsibilities

When asked how responsibilities are divided among players in the AI space, Frédérique identified two main groups:

- developers and suppliers: organizations that build foundation models, specialized models and technical infrastructure needed to create and deploy AI systems. They play a key role in ensuring the quality and origin of AI system training data and designing built-in safeguards. Developers and suppliers also provide adequate transparency, including technical documentation and disclosures on the limitation of their AI system.

- users and purchasers: organizations that integrate and roll out AI tools, such as chatbots, analytical tools and decision support systems, in their day-to-day operations. They are chiefly responsible for configuring and tailoring the AI system to their needs and managing the data they share with the AI system (e.g., the contents of chatbot queries). Users and purchasers are also responsible for implanting internal controls and monitoring, and reviewing how these tools impact privacy, security and equity.

Depending on the business environment, governance expectations can vary significantly.

- B2B solutions (businesses): The parties' responsibilities are generally set out in detailed commercial agreements that include provisions on governance, auditing, security, AI model lifecycle management, and contractual liability. While shaped by the regulatory framework, these agreements often go well beyond the minimum legal requirements.
- B2C solutions (consumers): Given the asymmetry in the relationship between the parties, users rarely get a say in the contract terms. As a result, the prevailing regulatory framework and consumer protection laws generally provide the main guidelines for these solutions. Both suppliers and purchasers may be subject to higher regulatory and societal expectations, particularly when it comes to transparency, privacy safeguards, equity and how risks to individuals are managed.

Currently, international governance frameworks (such as the *EU Artificial Intelligence Act* and National Institute of Standards and Technology [NIST] guidelines) mostly focus on high-risk AI systems used in fields like healthcare, education, recruiting and the administration of justice. This means most business use cases — often viewed as posing a low to moderate level of risk — remain subject to more limited regulatory oversight.

However, this is a rapidly changing landscape, and it is likely legislators and regulators will refine or broaden oversight as new uses of AI emerge.

Global standardization and regulation

Internationally, the AI regulatory environment remains fragmented. Some regions, finding the balance between innovation and risk elusive, have backtracked on legislation. Against this backdrop, the European Commission recently put forward the *Digital Omnibus on AI Regulation Proposal*. This proposal introduces "targeted simplification measures to ensure timely, smooth, and proportionate implementation of certain of the *AI Act*'s provisions." If adopted, these measures would postpone the entry into application of certain *EU AI Act* requirements for high-risk AI systems until 2027 and, in some cases, 2028.

In the Asia-Pacific region, Japan and South Korea are enacting broad-based legislation that ties together security, innovation, economic investment and training. The key objective of these countries is to promote responsible AI adoption while strengthening global competitiveness.

Canada does not currently have a dedicated legal framework governing AI. The government of Canada is prioritizing responsible adoption over strict regulation.

The federal Minister of Artificial Intelligence and Digital Innovation is planning to overhaul the country's privacy protection framework by updating the *Personal Information Protection and Electronic Documents Act* (PIPEDA). This reform would not create an AI-specific regulatory framework, unlike former Bill C-27's proposed *Artificial Intelligence and Data Act*, which died on the order paper at the dissolution of the previous parliament.

In parallel, Innovation, Science and Economic Development Canada (ISED) recently set up an AI Strategy Task Force and kicked off public consultations to help shape Canada's AI strategy.

As part of these consultations, Osler held an interactive online workshop on its AccessPrivacy platform. In attendance were two task force members from its safety and public trust working group: Joelle Pineau, Chief AI Officer, Cohere, and Doyin Adeyemi, JD/MBA candidate, University of Toronto, Fellow 1834. The recording of the workshop was provided to the minister.

Conclusion: toward Integrated AI and privacy governance

The conversation with Frédérique confirms that privacy laws and business strategy are deeply linked with advances in AI.

For organizations to manage these areas successfully, legal teams should keep informed about new technologies and how they are being used in their company. Developments in AI and privacy regulations should be tracked, both in Canada and abroad. Organizations should build their risk management approach around three core components: readiness, coordination and governance.

> Adopting AI without strong governance is not an option for organizations looking to maintain trust and keep emerging risks under control.
>
> ***Frédérique Horwood***

[1] For example, see the OWASP Top 10 for Agentic Applications for 2026.