JANUARY 16, 2025 • 10 MIN READ

Looking ahead: the Canadian privacy and AI landscape without Bill C-27

AUTHORS

 Nic Wall

 Molly Reynolds

 Rosalie Jetté

 Julie Himo

 Lauren Nickerson

 Mavra Choudhry

Further reading:

- Forging your AI path: Resources for business leaders
- AI will not be judging you: Canadian Judicial Council issues guidance on the use of AI in Canadian courts

With the prorogation of Parliament last week, Bill C-27, including the new AI law and proposed privacy reforms it contained, “died”. No new federal privacy or AI legislation is likely to pass anytime soon. However, privacy and AI standards—and therefore risks of non-compliance—continue to evolve. This bulletin surveys the privacy and AI landscape with Bill C-27 no longer on the horizon.

What you need to know

- While no new federal privacy or AI legislation is likely to pass this year, Canadian organizations should continue to monitor the constantly evolving privacy and AI landscape.
- Recent provincial reforms in Québec and elsewhere are likely to continue impacting organizations as this evolution informs industry standards, even for businesses with limited operations in those provinces.
- Regulatory action and guidance indicate certain priority areas—including AI, biometrics, deceptive design practices, and protection of children’s and health information—that are likely to receive increased investigative scrutiny.
- Trends in class action litigation indicate increasing risk associated with intentional data use and AI initiatives.
- International laws and standards also influence practices, expectations and risks in the Canadian market.

Provincial laws

Québec

Québec's *Act respecting the protection of personal information in the private sector* (Law 25), the final component of which came into force in September 2024, will continue to be a major influence on privacy requirements for several reasons. First, Law 25 contains the most significant penalty provisions of any privacy law in Canada—up to $10 million or 4% of an organization's global revenue. It also has a broad potential scope of extraterritorial application, and contains some of the most stringent and prescriptive requirements.

In light of these factors, many organizations have elected to apply Québec's standards and rights to all data subjects, even when those data subjects are located outside of Québec. Some of these organizations prefer a single, harmonized set of requirements; others lack an effective means of identifying a data subject's province and delineating their processes accordingly. In some cases, organizations that were not subject to Law 25 also chose to adopt Québec-compliant practices, with the objective of gaining a competitive advantage and fostering important business relationships with partners who are subject to Law 25. We therefore expect to see Law 25 continue to influence industry practice, even when the law does not directly apply in the circumstances.

Ontario

The June 2021 release of the Ontario government's white paper on privacy reform[1] was accompanied by comments from the then-Minister of Government and Consumer Services indicating that if federal privacy reform was insufficient, the Ontario government would possibly step in. There have been no public statements indicating this intention recently.

However, the Ontario government has shown recent willingness to legislate on both privacy and AI. In November, the government passed the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*. This Act creates new regulation-making powers regarding public sector cybersecurity and use of AI. Another component of this reform would, once proclaimed, expand the Ontario Information and Privacy Commissioner's investigative powers with respect to public institutions. Ontario has also passed legislation that, once in force, would require employers to disclose the use of AI in their hiring process.

Alberta

Alberta recently passed reforms to its public sector privacy law, the *Freedom of Information and Protection of Privacy Act*, with the enactment of Bill 33. Bill 33, the *Protection of Privacy Act*, includes strengthened privacy protections and new rules with respect to data use and sharing. It also includes increased penalties (up to $750,000 for an organization), which the Alberta government is hoping will give some teeth to a statute that had not been looked at in over two decades.

While Alberta's private sector privacy law, the *Personal Information Protection Act* (PIPA) is still currently under review, the approach taken by the government for the public sector legislation, as well as the support it has received from the provincial privacy commissioner, may indicate an appetite for private sector reform, too.

Regulatory action and guidance

Regulatory action and guidance continue to influence standards in privacy and AI. For example, in December 2023, the Office of the Privacy Commissioner of Canada (OPC), jointly with all Canadian provincial and territorial privacy regulators, released guidance on generative AI entitled *Principles for responsible, trustworthy and privacy-protective generative AI technologies.* Our summary of this guidance is available here.

Other recent actions by OPC and other privacy regulators can be taken as indicative of enforcement priorities. In addition to the use of generative AI, these include:

- children's privacy;
- biometrics;
- deceptive design practices;
- collection and use of data for AI training;
- protection of personal health information; and
- employee surveillance.

Privacy concerns regarding these topics will be subject to higher degrees of regulatory scrutiny. This heightened regulatory risk in turn creates heightened litigation and reputational risk.

Many other regulators have also taken actions that indicate AI will be subjected to heightened scrutiny. For example, the Competition Bureau has signaled its intention to continue monitoring the use of AI and its impact on competition, and identified concerns about certain potential uses of AI including algorithmic pricing, algorithmic collusion, and the use of deepfakes. Human rights watchdogs, such as the Ontario Human Rights Commission, have flagged the potential for bias and discrimination in AI systems. Furthermore, the Office of the Superintendent of Financial Institutions and the Financial Consumer Agency of Canada recently released a joint report on the risks of AI in federally regulated financial institutions[2].

Generally, Canadian regulators have emphasized the importance of cross-sector collaboration given the complex and multifaceted nature of AI regulation, particularly in the areas of privacy, competition, telecommunications, and intellectual property.

Class action litigation

Privacy class actions

Broadly speaking, the last few years have seen an increasingly sophisticated class action plaintiffs' bar expand beyond class action claims based on data breaches to include an organization's intentional data handling practices. For example, claims may be based on an allegation of the collection, use, or disclosure of personal information without sufficient consent. Such data handling claims can be based in tort, contract or statute. Ultimately, this means that the litigation risk for data handling practices involving a large number of individuals is higher than it was several years ago, and continues to increase.

AI class actions

The intersection of AI and class action litigation is also growing. Such class actions include:

- privacy-related claims, such as the use of AI to improperly obtain biometric identifiers of individuals;
- employment and discrimination-related claims, such as discrimination in the hiring process stemming from the use of AI;
- anti-trust and competition-related claims, such as the use of AI leading to price-fixing or market manipulation;
- insurance-related claims, such as the improper use of AI to make insurance claim determinations; and
- intellectual property-related claims, such as the unlicensed use of copyrighted material to train AI systems.

Our summary of the growing intersection of AI and class action litigation is available here.

International AI laws and standards

International laws can be influential in setting standards and expectations, particularly for organizations operating in multiple jurisdictions that seek a harmonized privacy or AI governance program. Note, however, that in the absence of major changes to the international privacy landscape, this section focuses on AI laws and standards.

European law

The European Union's *Artificial Intelligence Act* (AIA) is a prime example. The AIA came into force in August 2024 and is set to take effect incrementally over the next two years. The AIA imposes obligations pertaining to risk management, data governance, documentation and record-keeping, human oversight, cybersecurity, transparency, and quality control, among others. Its scope of application includes providers and deployers of AI systems located outside the EEA whose AI outputs are used within the EU. This means that, like the EU's data privacy regulations (known as the GDPR), the AIA can apply to Canadian businesses with operations or customers in the EEA. Over the last several years, the GDPR has had a significant impact on global privacy practices and the AIA is expected to be similarly influential on AI standards.

United States law

There is currently no proposed comprehensive federal AI-specific legislation in the U.S. In 2023, the Biden White House issued an executive order concerning the safe and secure use of AI that addressed privacy, security, equity, and human rights concerns, but the incoming Trump administration has signaled its intention to both repeal this order and oppose regulation that could interfere with AI innovation. However, as in privacy law, a patchwork of state AI laws is emerging. Three states have been leading the pack for legislation governing the private sector: Utah, Colorado and California. These three states adopted legislation in 2024 which include requirements with respect to governance and transparency related to the use of AI.

In addition, Illinois, Massachusetts and Ohio have several active bills that are currently being reviewed at the committee level.

Other jurisdictions

The United Kingdom's government recently announced its intention to introduce AI legislation, which is anticipated sometime this year.

The South Korean National Assembly recently passed the *Basic Act on the Development of Artificial Intelligence and the Establishment of Trust*, which will take effect in January 2026. Taiwan, Brazil, and Chile have also introduced draft AI legislation. Like the AIA, each of these instruments will impose different regulatory obligations based on an AI system's presumed level of risk.

International standards

In 2023, the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce, published a voluntary set of guidelines titled the *AI Risk Management Framework*, with the goal of managing AI-related risk and increasing trustworthiness in the design, development, and use of AI systems.

The International Standards Organization has also released certain standards, including ISO/IEC 42001, 23894, and 38507. ISO/IEC 42001, released in December 2023, specifies requirements for establishing, implementing, maintaining, and continually improving an AI management system to help ensure responsible development and use.

While these international standards are non-binding, they can nevertheless inform expectations. Businesses may inquire about compliance with such standards as part of a due diligence exercise, or contractually require compliance when acting as a customer for an AI-based product or service. Moreover, these standards have the potential to indirectly inform legal obligations, such as a company's standard of care in a negligence claim.

Implications for businesses

The privacy and AI landscape continues to rapidly evolve, even in the absence of Bill C-27. Canadian organizations should continue to monitor this landscape, particularly given the pace of change.

For the sake of efficiency, many organizations were delaying some of their privacy and AI compliance initiatives until the requirements of Bill C-27 crystallized. However, with Bill C-27 no longer on the horizon, organizations should revisit their compliance initiatives to identify and address key risk areas, and establish a list of priorities for 2025. For privacy compliance, special attention should be paid to Law 25 requirements and recent regulatory actions and decisions. AI governance programs should align with best practices to help limit risk, meet existing industry expectations and reduce the compliance burden as new AI laws are passed.

FOOTNOTES

1. Government of Ontario, Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy, June 2021.
2. Office of the Superintendent of Financial Institutions, OSFI-FCAC Risk Report: AI Uses and Risks at Federally Regulated Financial Institutions. September 24, 2024.

To discuss these issues, please contact the author(s).