Do you know what your neighbour is doing? AI developments in Canada and the United States

Grow | Protect | Operate | Finance

August 2023

With the recent and rapid rise of generative artificial intelligence (AI), there have been new calls for AI regulation. Although a consensus is building that comprehensive and coordinated AI regulation is a necessity, how that regulation will develop remains an open question. At the time of this writing, there are currently over 800 AI policy initiatives in 69 countries around the world. Below we highlight two of those jurisdictions – Canada and the United States (US). We also provide key takeaways for organizations to leverage as they look to address AI risk at an enterprise level.

Canada

In Canada, there are several rules in effect today that impact AI and several others in various stages of proposal:

Existing rules

- **Québec Law 25**: This law governs automated decision-making systems using personal information. Law 25 takes effect in September 2023, will impose transparency obligations with respect to personal information used in decisions made exclusively by automated processing, and will provide a data subject the right to have those decisions reviewed by a human. Québec's regulator, the *Commission d'accès à l'information*, will enforce the law and have the ability to impose administrative monetary penalties of up to CA$10 million or 2% of worldwide turnover.
- **Federal directive on automated decision-making**: This federal directive applies to all federal institutions and requires an algorithmic impact assessment prior to the implementation of any automated decision system. The directive also imposes transparency and quality assurance obligations, and requires the institution to provide recourse to challenge decisions. Organizations who seek to provide automated decision-making services or products to Canada's federal government must also comply with the directive.

Proposals

- ***Amended Personal Information and Protection of Electronic Documents Act:*** Bill C-27 introduces a successor piece of legislation to the federal *Personal Information and Protection of Electronic Documents Act*. It would impose transparency and data subject obligations relating to automated decision-making systems used to assist human decision-makers.

- ***Artificial Intelligence and Data Act:*** Bill C-27 would introduce this law that, if passed, would, in respect of "high-impact" AI systems, require organizations to implement risk management and mitigation practices relating to the use of AI, impose transparency obligations on the use of AI and require reporting to regulators.

United States

In the United States, it's a more complicated landscape. A patchwork of federal and state efforts are developing around regulating the development and deployment of AI.

Federal policy developments

The earliest signs of a federal AI strategy in the US were outlined during the Obama administration, including a public report issued by the National Science and Technology Council in October 2016, Preparing for the Future of Artificial Intelligence. Federal strategies and proposed AI governance frameworks have since evolved:

- The Obama administration released the National Artificial Intelligence Research and Development Strategic Plan, updated in 2019 and 2023.

- The Trump administration signed Executive Order 13859, titled Maintaining American Leadership in Artificial Intelligence.

- In October 2022, the Biden administration's Office of Science and Technology Policy released a proposed blueprint for an AI Bill of Rights with five guiding principles, including (1) creating safe and effective AI systems; (2) protecting against algorithmic discrimination; (3) enhancing data privacy; (4) ensuring adequate notice and transparency; and (5) examining human alternatives.

- In February 2023, the White House issued an Executive Order that directs federal agencies to root out bias in their design and use of AI to protect the public from algorithmic discrimination.

- In May 2023, the White House Office of Science and Technology Policy issued a Request for Information, seeking public input on "mitigating AI risks, protecting individuals' rights and safety, and harnessing AI to improve lives[.]"

- On May 4, 2023, the White House held a high-level meeting with the CEOs of AI companies and announced new actions to promote responsible innovation in AI, including new investments in AI research and development, public assessments of existing generative AI systems, and policies to ensure the federal government is mitigating AI risks and harnessing AI opportunities.

- In June 2023, President Biden issued a statement on AI, noting: "My administration is committed to safeguarding America's rights and safety, from protecting privacy to addressing bias and disinformation and making sure AI systems are safe before they are released[.]"

- In July, the White House announced it had secured "voluntary commitments" from seven leading AI companies to behave "responsibily" and ensure their products are "safe" when deployed. Shortly after that meeting, Anthropic, Google, Microsoft, and OpenAI announced the formation of the new Frontier Model Forum to advance AI safety research, amongst other activities.

Federal agency developments

Federal agencies are also taking steps to regulate the development and deployment of AI.

- In April 2022, the Department of Energy's AI Intelligence and Technology Office developed an AI Risk Management Playbook in consultation with the National Institute of Standards and Technology (NIST) and the AI Advancement Council.

- In May 2022, the Equal Employment Opportunity Commission (EEOC) and US Department of Justice (DOJ) issued technical assistance guidance outlining their enforcement position and recommendations as it relates employer use of AI and the *Americans with Disabilities Act* (ADA). In May 2023, the EEOC released additional resources on AI and Title VII.
- In 2022 and 2023, the Department of Commerce's US Patent and Trademark Office created an AI/emerging technologies page and group to study the impact of AI on patent and trademark examination.
- In January 2023, the Department of Commerce's NIST released an AI risk management framework to help organizations better handle AI-related threats.
- In April 2023, the Department of Commerce's National Telecommunications and Information Administration launched a Request for Comment to shape a comprehensive federal government approach to AI-related risks and opportunities.
- On April 25, 2023, the DOJ, EEOC, Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) issued a joint statement on their efforts to regulate the use of AI through existing legal authorities under the *Civil Rights Act of 1964*, the *FTC Act* and other federal statutes.
- The FTC has repeatedly provided guidance on AI tools since 2020, and is focused on scrutinizing the use of generative AI that may unfairly steer individuals into harmful decisions. Most recently, the FTC has launched an investigation into OpenAI and has publicly discussed the risk of AI and its impact on consumer trust.

Federal congressional developments

At the federal congressional level, there have been a number of efforts in recent years to address AI in various industries. Below is a sample of those proposals, which are still in bill form:

- S. 3572, the *Algorithmic Accountability Act of 2022*, would authorize the Federal Trade Commission to require companies under its jurisdiction to study and address potential unfair bias and discrimination in algorithms.
- HR 3611, the *Algorithmic Justice and Online Platform Transparency Act*, would make it unlawful to use AI on an online platform in a manner that deprives an individual of rights under the *Civil Rights Act of 1964*.
- HR 3044 would amend the *Federal Election Campaign Act of 1971* to provide more transparency and accountability around the use of generative AI in political advertisements.
- HR 0066 encourages congress to focus on regulating AI in a safe and ethical manner.
- S. 262, the *Stop Spying Bosses Act*, would prohibit employers from engaging in workplace surveillance using automated decision systems.
- HR 8152, the *American Data Privacy and Protection Act*, would require impact assessments around the use of AI systems if they are used in a manner that poses a "consequential risk of harm to an individual or group of individuals."
- S. 2024, the *Filter Bubble Transparency Act*, would apply new requirements on platforms that use "algorithmic ranking systems," including computational processes derived from AI.
- S. 3195, the *Consumer Online Privacy Rights Act*, would regulate "algorithmic decision-making" amongst other issues relating to AI.
- On May 16, 2023, the Senate Judiciary Committee's Subcommittee on Privacy, Technology, and the Law and the Senate Homeland Security and Governmental Affairs Committee held public hearings to discuss AI issues.
- In June 2023, Senator Charles Schumer (DNY) announced the creation of the SAFE Innovation Framework to help guide Congress in developing AI regulations. As part of this process, the Senate will invite AI experts to convene a series of "AI Insights Forums" for a "new and unique approach to developing AI legislation."
- On July 25, the Senate Judiciary Committee Subcommittee on Privacy, Technology, and the Law held an additional hearing on AI regulation.

US state developments

Lawmakers in a number of US states have also introduced bills and passed various types of legislation aimed at regulating various aspects of AI.

- **California**: The *Bolstering Online Transparency Act* took effect in 2019 and makes it unlawful for any person or entity to use an artificial bot to communicate with a person in California in order to incentivize a sale or transaction of goods or services, or to influence a vote in an election without disclosing its existence as a bot. California likewise addresses automated decision-making and profiling under the *California Consumer Privacy Act*, as amended by the *California Privacy Rights Act*.
- **Connecticut**: The *Connecticut Privacy Act* took effect on July 1, 2023, and provides Connecticut consumers the right to opt out of profiling if such profiling is furtherance of automated decision-making that produces legal or other similarly significant effects.
- **Colorado**: In 2021, Colorado enacted the *Protecting Consumers from Unfair Discrimination in Insurance Practices Act*, which prohibits the use of "algorithms and predictive models" by the insurance industry that unfairly discriminate based on race, gender, sexual orientation and other factors. The *Colorado Privacy Act* also took effect on July 1, 2023, providing Colorado consumers the right to opt out of profiling if such profiling is in furtherance of automated decision-making that produces legal or other similarly significant effects.
- **District of Columbia**: B114, the *Stop Discrimination by Algorithms Act of 2023*, would if adopted prohibit organizations from using algorithms that make decisions based on protected personal traits.
- **Illinois**: In 2019, Illinois became the first state to impose restrictions on the use of AI when hiring under the Illinois *AI Video Interview Act*, which requires covered employers to provide notice, explanation and obtain consent around the use of AI in interviews.
- **Indiana**: The *Indiana Consumer Data Protection Act*, which takes effect January 1, 2026, sets out rules for profiling and automated decision-making.
- **Maine**: The *Data Privacy and Protection Act* is a bill that was introduced in May 2023, and would impose specific restrictions on the use and deployment of algorithms, including the duty to perform risk assessments.
- **Maryland**: HB 1202 took effect on October 1, 2023, and prohibits employers from using facial recognition services for the purpose of creating a facial template during an applicant's pre-employment interview unless the employer obtains express consent.
- **Massachusetts**: Massachusetts has several bills pending that would impact AI. The proposed *Massachusetts Data Privacy Protection Act* and Massachusetts Information Privacy and Security Act would each impact automated decision-making, and impose impact assessments when using covered "algorithms." H1873 would require employers provide employees and independent contractors with notice prior to the use of an automated decision system and the right to request certain information about such use. And SB31 would require any company operating a large-scale generative AI model to adhere to certain operating standards as reasonable security measures, as well as the performance of regular risk assessments.
- **Montana**: The *Montana Consumer Data Privacy Act* takes effect on October 1, 2024, and sets out rules around profiling and automated decision-making.
- **New Jersey**: Bill A4909 would regulate the use of automated tools in making hiring decisions. A537 would require an automobile insurer using an automated or predictive underwriting system to annually provide documentation and analysis to the Department of Banking and Insurance to ensure against discriminatory outcomes in the pricing based on a protected characteristic. S1402 would prohibit automated decision systems from discriminating against individuals based on a protected class as it relates to obtaining financial products, insurance products or healthcare.

- **New York**: New York City passed the first law in the US requiring employers to conduct bias audits of AI-enabled tools used for employment decisions. New York has also introduced the *New York Privacy Act*, which would require certain disclosures around automated decision-making.
- **Oregon**: The Oregon Consumer Privacy Act provides certain rules concerning profiling that may involve automated decision-making.
- **Pennsylvania**: HB49 would direct the Department of State to establish a registration of businesses using AI systems.
- **Rhode Island**: SB146 would prohibit certain uses of automated decision systems and algorithmic operations in connection with video-lottery terminals and sports betting applications.
- **South Carolina**: SB404 would prohibit any operator of a website or other online service to utilize an automated decision system for content placement, posts, advertisements or product offerings for users under the age of 18.
- **Tennessee**: The *Tennessee Information Protection Act* takes effect July 1, 2025, and requires data impact assessments associated with certain types of profiling that may involve automated decision-making.
- **Texas**: The *Texas Data Privacy and Security Act* takes effect July 1, 2024, and creates requirements to allow Texas residents to opt out of the profiling of the individual using automated decision-making, amongst other requirements.
- **Vermont**: H114 would restrict the use of electronic monitoring of employees and the use of automated decision systems for employment-related decisions.
- **Virginia**: The *Virginia Consumer Data Protection Act* took effect on January 1, 2023, and sets out rules as it relates to the right to opt out of profiling using automated decisions, amongst other requirements.

Key takeaways

Regardless of the statutory or regulatory framework being deployed, regulators and stakeholders across the US and Canada are beginning to coalesce around a singular approach to governing AI – requiring organizations to engage in “responsible” or “trustworthy” use of AI.

Although there is no single definition of “responsible” or “trustworthy” AI, we are beginning to see certain principles develop. Those principles are derived from multiple frameworks, but can generally be broken down as being: (1) valid, reliable and robust; (2) safe, secure and resilient; (3) transparent, explainable, and interpretable; and (4) privacy-enhanced and fair.

Below we outline key features of these principles, and provide an overview of how Dentons can help your organization leverage these principles to build a robust AI risk management framework to mitigate risk and maximize opportunity when leveraging generative AI or other AI systems.

Responsible AI principles

Principle #1 - Valid, reliable and robust

Valid refers to confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application of the AI system are fulfilled. ***Reliable*** refers to the ability of an AI system to perform as required, without failure, for a given time interval, under given conditions. ***Robust*** refers to the ability of an AI system to maintain its level of performance under a variety of circumstances.

Principle #2 - Safe, secure and resilient

AI systems should be ***safe*** in that they should not lead to a state in which human life, health, property or the environment is endangered. AI systems should also be ***resilient*** and ***secure*** - that is, they can withstand unexpected adverse events or unexpected changes in their environment or use and involve security features that prevent against security threats and challenges. Common security challenges with AI systems include data poisoning, exfiltration of models, training data compromise or other AI endpoint vulnerabilities.

Principle #3 - Transparent, explainable and interpretable

Transparent reflects the extent to which information about what occurred within an AI system and its outputs is made available to impacted stakeholders. Transparency may involve disclosing information about an AI system's design decisions, training data, structure, intended uses, deployment plan, end-user decision options and potential adverse outcomes. ***Explainable*** refers to a representation of the functions of an AI system. ***Interpretable*** refers to the meaning of an AI system's output in the context of its designed functional purpose. In other words, transparency answers "what happened" within an AI system, explainability answers "how" a decision was made and interpretability explains "why" a decision was made.

Principle #4 – Privacy-enhanced and fair

Privacy-enhanced values such as anonymity, confidentiality and integrity should be built into AI systems throughout the system lifecycle. Privacy-enhanced technologies for AI, as well as data minimization principles such as de-identification and aggregation for certain model outputs, should also be considered. ***Fairness*** in AI includes concerns for equality and equity. Standards of fairness can be complex and difficult to define and determining what is an acceptable threshold for "fair" for any organization is context specific. At a baseline, however, the AI system should not result in discrimination prohibited under applicable law.

What next?

To guide your organization in developing your own AI risk management framework based on the above principles (or those that your organization developments), we recommend thinking through the following steps:

Guidance and oversight	• **Establish** a cross-functional committee or group comprised of stakeholders across the enterprise to run point on developing responsible AI principles and governance structures. • **Advise** the enterprise on AI risk management, implementation of the responsible AI principles and operationalizing awareness throughout the enterprise on the approach to responsible AI.

Policies and procedures	• **Develop** and adopt a set of responsible AI principles. Each organization must agree upon and develop its own principles and reflect those principles in a written policy. • **Develop** and adopt acceptable use policies to address immediate usage of generative AI tools by stakeholders who may present a direct risk, and to facilitate immediate opportunities. Dentons Canada has developed a comprehensive, ready-to-use Canadian Generative AI Policy template that can be easily integrated into your employee policy handbook as is and/or with updates to add scenarios specific to your organization, located in Canada. We are pleased to make this available to any employer who requires such a policy for a flat fee of CA$1000 (exclusive of taxes). Reach out to the Dentons lawyer you usually work with, or request your Generative AI Policy template policy here.
Controls	• **Implement** policy, technical and organizational controls to align with the mapping and measuring of AI risk. • These controls must be **developed** through each department. • Controls must be **balanced** to mitigate risk but capture opportunity.
Incident management	• **Ensure** deployment of AI is incorporated into existing incident response processes to mitigate risk. • Through the mapping and measuring processes, **build** in AI risk mitigation measures to present incidents. Test those processes.

Dentons recently published a white paper entitled "The Future of AI Governance" examining the future of AI regulation and offering a new way of thinking about how AI regulation could be scalable to take into accountt he trajectory of AI. To learn more, download a copy of the paper here.

Contact Us

To learn more about how Dentons can help with your business needs in the US, please reach out to Peter Stockburger, and in Canada, Luca Lucarini.

CSBrand-122740-AI Flyer_06 — 09/08/2023