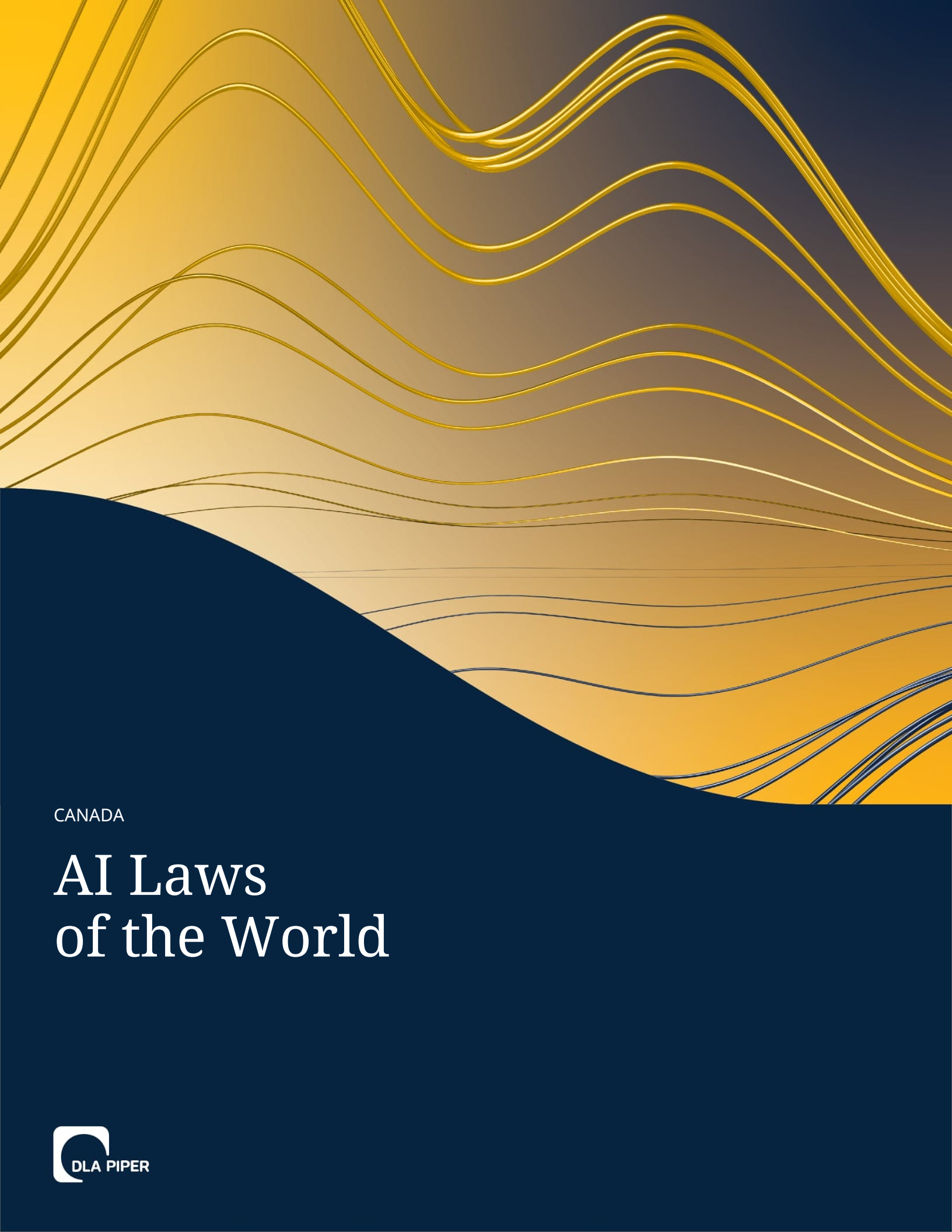




CANADA

AI Laws of the World

Introduction



Artificial intelligence (AI) is rapidly transforming the way we work. As AI technology advances, governments are grappling with how to regulate its development to maximise benefits whilst mitigating risks.

Some jurisdictions have implemented AI-specific laws, whilst others are in the process of drafting regulations, and many rely on existing legal frameworks to address AI-related concerns.

This guide provides an overview of AI laws and proposed regulations across 50+ territories. It highlights key legislative developments, including regulations, proposed bills and guidelines issued by governmental bodies.

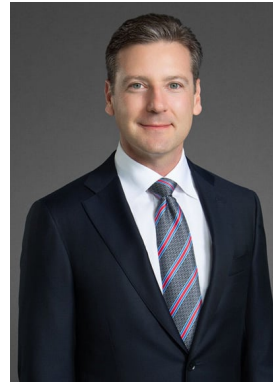
As the global landscape of AI regulation evolves at an accelerating pace, our 2026 Q3 snapshot provides an insightful overview of these developments, as well as of the common thematic approaches of lawmakers and AI-focused organisations around the world.

Global key contacts



Gareth Stokes

Partner
Global Co-Chair, AI Practice
gareth.stokes@dlapiper.com
[Full bio](#)



Danny Tobey

Partner
Global Co-Chair AI and
Data Analytics
danny.tobey@us.dlapiper.com
[Full bio](#)



Law / proposed law

AI-specific laws have not yet passed in Canada at the federal level. In June 2026, the federal government launched 'AI for All', Canada's new national AI strategy, which sets out six pillars covering protecting Canada and democracy, empowering Canadians, powering prosperity, sovereign AI infrastructure, scaling Canadian AI, and international partnerships. It identifies five priority sectors: health and life sciences, energy and natural resources, transportation, agriculture, and manufacturing and robotics. The strategy is presented as a five-year plan, with 'trust' described as its 'north star' and a stated goal of increasing Canadian business AI adoption from 12% to 60% by 2034. While the strategy does not itself introduce new AI-specific legislation, it signals the government's ongoing commitment to developing a comprehensive regulatory framework for AI.

An Artificial Intelligence and Data Act (**AIDA**) was proposed as part 3 of Bill C-27 in June 2022, with the stated purpose of regulating AI systems in interprovincial and international trade and prohibiting certain conduct that may result in serious harm. AIDA died on the order paper in January 2025 when Prime Minister Trudeau prorogued government. The bill faced criticism for being part of a sweeping privacy omnibus and for deferring key details to regulations, which limited parliamentary focus on AI-specific issues. AIDA had also drawn significant criticism from Canada's technology sector as potentially more restrictive than the European Union's *Artificial Intelligence Act*—an approach seen as untenable for a middle power seeking to attract and retain AI companies.

Perhaps in response, the 2026 'AI for All' strategy does not signal any intention to reintroduce standalone AI legislation comparable to AIDA. Instead, AI-related risks are expected to be addressed through targeted legislation, including promised privacy modernisation (see Bill C-36 introduced 15 June 2026) and online safety (see Bill C-34 introduced 10 June 2026) legislation, rather than through a single comprehensive regulatory framework.

Although there is no AI-specific federal legislation, AI-related rules appear in provincial legislation and federal privacy law. At the provincial level:

- Quebec's *Act respecting the protection of personal information in the private sector* (as amended by 'Law 25') imposes transparency and disclosure obligations on organisations that use personal information to render a decision based exclusively on automated processing. Individuals may request information about the personal information used, the reasons for the decision, and their right to have the information corrected.
- As of January 2026, Ontario's *Employment Standards Act, 2000* requires employers that advertise publicly-advertised job postings to disclose to applicants when they implement AI to screen, assess, or select applicants (see [Ontario confirms new regulations addressing pay transparency and job posting requirements](#)).
- In November 2024, Ontario passed the *Enhancing Digital Security and Trust Act, 2024* (EDSTA), establishing public sector transparency, accountability, and risk management frameworks for the use of AI. Regulations under EDSTA take effect on 1 July 2026. Ontario's Responsible Use of Artificial Intelligence Directive, effective since December 2024, also sets requirements for AI risk management and transparency across Ontario ministries and provincial agencies.
- British Columbia has appointed a Minister of State for Artificial Intelligence and New Technologies, with a mandate to engage on federal AI law and policy development and to promote AI adoption by BC businesses.
- At the federal level, on 10 June 2026, the Government of Canada introduced Bill C-34, the *Safe Social Media Act*, for First Reading in the House of Commons. The bill proposes sweeping new legislation to regulate social media platforms, AI-powered chatbot services, and other online services operating in Canada. The bill's centrepiece is a temporary prohibition on social media accounts for persons under age 16, backed by age-verification obligations. It also introduces broad content-moderation duties, new obligations specific to AI chatbot services (including crisis intervention requirements and a prohibition on chatbots posing as humans), and a new independent regulator, the Digital Safety Commission of Canada, with substantial investigatory and enforcement powers. If enacted, Bill C-34 would represent one of the first frameworks globally to treat chatbot services as a distinct statutory category with tailored duties.

Regulatory guidance / voluntary codes

In September 2023, the Canadian Minister of Innovation, Science and Industry announced a [Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems \(Voluntary Code\)](#) to provide Canadian companies with common standards until formal regulation is in effect, with the aim of enabling them to demonstrate voluntarily that they are developing and using generative AI systems responsibly. The Voluntary Code sets out identified measures to which companies must adhere when nominating themselves as signatories to it relating to the following:

- **Accountability** – Firms understand their role with regard to the systems they develop or manage, put in place appropriate risk management systems, and share information with other firms as needed to avoid gaps.
- **Safety** – Systems are subject to risk assessments, and mitigations needed to ensure safe operation are put in place prior to deployment.

- **Fairness and Equity** – Potential impacts with regard to fairness and equity are assessed and addressed at different phases of development and deployment of the systems.
- **Transparency** – Sufficient information is published to allow consumers to make informed decisions and for experts to evaluate whether risks have been adequately addressed.
- **Human Oversight and Monitoring** – System use is monitored after deployment, and updates are implemented as needed to address any risks that materialize.
- **Validity and Robustness** – Systems operate as intended, are secure against cyber attacks, and their behaviour in response to the range of tasks or situations to which they are likely to be exposed is understood.

The level of obligation in respect of each of the measures to be undertaken varies depending on whether a signatory is either a developer or a manager of a generative AI system and whether or not the system is available for public use or not.

In December 2023, Canadian privacy regulators announced Principles for responsible, trustworthy and privacy-protected generative AI technologies (**Privacy Principles**) to help organisations that are developing, providing, or using generative AI technologies apply key Canadian privacy principles:

- **Legal Authority and Consent** – Organisations should ensure they have legal authority for collecting and using personal information (and when consent is the legal authority, it should be valid and meaningful).
- **Appropriate Purposes** – Organisations should only collect, use, and disclose personal information for appropriate purposes.
- **Necessity and Proportionality** – Organisations should establish the necessity and proportionality of using generative AI, and of personal information within generative AI, to achieve the intended purposes.
- **Openness** – Organisations should be open and transparent about the collection, use, and disclosure of personal information and the potential risks to individuals' privacy.
- **Accountability** – Organisations should establish accountability for compliance with privacy legislation and principles and make AI tools explainable.
- **Individual Access** – Organisations should facilitate individuals' right to access their personal information by developing procedures that enable it to be meaningfully exercised.
- **Limiting Collection, Use, and Disclosure** – Organisations should limit the collection, use, and disclosure of personal information to only what is needed to fulfil the explicitly specified, appropriate identified purposes.
- **Accuracy** – Organisations should ensure that personal information is as accurate, complete, and up-to-date as is necessary for purposes for which it is to be used.
- **Safeguards** – Organisations should establish safeguards to protect personal information and mitigate potential privacy risks.

Appointed supervisory authority

A supervisory body with authority for AI has not yet been appointed in Canada by way of statutory appointment. For the deployment of AI in the public sector, the federal government has committed to establishing an AI Centre of Expertise on project support, knowledge sharing, and strategic guidance to support AI adoption and experimentation. In November 2025, the federal government launched its first register of AI uses in federal government, providing public transparency on how AI systems are deployed across federal departments and agencies. Bill C-34, if enacted, would establish the Digital Safety Commission of Canada as a new independent regulatory body with authority over regulated social media services and chatbot services. The Commission would be composed of three to five full-time members appointed by the Governor in Council, with renewable terms of up to five years. The Commission could issue compliance orders directing operators to take or refrain from specific actions, enforceable as Federal Court orders.

Definitions

National laws specifically addressing AI have not yet passed in Canada. The Privacy Principles differentiate between developers and providers (individuals or organisations that develop or train foundation models or generative AI systems, or that put such systems onto the market) and organisations using generative AI as part of their activities.

Prohibited activities

National laws specifically addressing AI have not yet passed in Canada. At the provincial level, using AI for screening and evaluating potential employees or using AI to make decisions based on personal information should be reviewed carefully.

High-risk AI

National laws specifically addressing AI have not yet passed in Canada.

Controls on generative AI

National laws specifically addressing AI have not yet passed in Canada. However, Bill C-34 (if enacted) would impose specific obligations on operators of 'regulated chatbot services', including requirements to mitigate the risk of communicating harmful content and to address specifically identified harmful behaviours. These provisions are discussed in the User transparency section. Canada's export control regime is primarily based on the multilateral Wassenaar Arrangement, which does not itself explicitly list AI in current control lists (though high-performance computing systems, encryption tools or network intrusion software, or certain imaging or machine vision sensors that may form part of AI technologies may meet criteria for control).

Due to stalls in global consensus on updating the Wassenaar Arrangement, on 20 July 2024, Canada unilaterally added certain quantum computing and advanced semiconductor technologies to its Export Control List, effectively prohibiting their export to any location other than the United States without an export permit. The list

of controlled goods specifically added is part of Export Control List Order SOR/2024-112, where the attached Regulatory Impact Analysis Statement mentions specifically the addition of gate-all-around field-effect-transistors/GAAFET based on their application in creating microchips that run faster and consume less power, thus enabling more powerful and efficient artificial intelligence applications, including for military systems.

Under Canada's national security powers under the *Investment Canada Act*, it is advisable to work with counsel to develop a strategy for managing the requisite notification to and/or review by government for all new businesses or acquisitions of business or other foreign direct or indirect investment where there is significant foreign control, to the extent they involve artificial intelligence resources. In April 2026, Innovation, Science and Economic Development Canada launched the Artificial Intelligence Sovereign Compute Infrastructure Program (SCIP), which provides funding for eligible Canadian-owned organisations to build or expand domestic AI compute capacity. The program forms part of the government's broader Sovereign AI Compute Strategy to reduce reliance on foreign AI infrastructure and support domestic AI development.

The 'AI for All' strategy also commits CAD 50 million to expand the Canadian AI Safety Institute to track emerging AI risks, advance technical research, and conduct transparent evaluations of AI models. It proposes creating a Canada Trusted AI Certification program to help Canadians identify trustworthy AI products in the marketplace. The government also intends to work on AI transparency initiatives, including tools such as watermarking AI-generated content.

Enforcement / fines

National laws specifically addressing AI have not yet passed in Canada. Bill C-34, if enacted, would establish a significant enforcement regime for regulated social media services and chatbot services. The Digital Safety Commission would have the power to impose administrative monetary penalties of up to 6% of global revenue or CAD 25 million (whichever is higher) for individuals and up to 8% of global revenue for corporations. The revenue-based penalty structure means that penalties scale with company size. The Commission could also issue compliance orders directing operators to take or refrain from specific actions, enforceable as Federal Court orders.

User transparency

National laws specifically addressing AI have not yet passed in Canada. Bill C-34, if enacted, would require operators of regulated chatbot services to ensure that chatbots that could be mistaken for humans are clearly and prominently identified as AI systems. Operators of regulated social media services would be required to label synthetic content (including deepfakes and AI-generated material) and to label content subject to automated bot amplification.

The Voluntary Code specifies under its Transparency principle that signatories should (with varying levels of obligation, as indicated, depending on whether a signatory is either a developer or a manager of a generative AI system and if the system is available for public use or not):

- publish information on capabilities and limitations of the system;
- develop and implement a reliable and freely available method to detect content generated by the system, with a near-term focus on audio-visual content (e.g., watermarking);
- publish a description of the types of training data used to develop the system, as well as measures taken to identify and mitigate risks; and
- ensure that systems that could be mistaken for humans are clearly and prominently identified as AI systems.

Chatbot-specific obligations

Bill C-34, if enacted, would impose specific obligations on operators of ‘regulated chatbot services’. Operators would be required to implement measures adequate to mitigate the risk that users will be exposed to or communicated harmful content. Operators must also mitigate the following specifically prohibited behaviours:

- posing as a human being in circumstances likely to lead a user to mistake the chatbot for a human;
- posing as a medical, legal, or other licensed professional and providing advice;
- using manipulative engagement techniques to encourage emotional attachment, leading to social withdrawal;
- encouraging self-harm, suicide, or acts causing death or serious bodily harm; and
- other behaviours as specified in regulations.
- Additionally, if a user expresses suicidal ideation, an intention to self-harm, or an intention to cause death or serious bodily harm to another person, the chatbot service must immediately interrupt the interaction and direct the user to crisis intervention services. The bill specifies that the crisis service must connect the user to a human being who is available at the time the user is directed towards them—automated crisis responses alone will not suffice.

The Privacy Principles specify that organisations that develop, provide, or use generative AI technologies must be open and transparent about the collection, use, and disclosure of personal information and the potential risks to individuals’ privacy.

Fairness / unlawful bias

The Voluntary Code specifies under its Fairness and Equity principle that signatories should (with varying levels of obligation, as indicated, depending on whether a signatory is either a developer or a manager of a generative AI system and if the system is available for public use or not):

- assess and curate datasets used for training to manage data quality and potential biases; and
- implement diverse testing methods and measures to assess and mitigate risk of biased output prior to release.

Human oversight

The Voluntary Code specifies under its Human Oversight and Monitoring principle that signatories to it should (with varying levels of obligation, as indicated, depending on whether a signatory is either a developer or a manager of a generative AI system and if the system is available for public use or not):

- monitor the operation of the system for harmful uses or impacts after it is made available, including through the use of third-party feedback channels, and inform the developer and/or implement usage controls as needed to mitigate harm; and
- maintain a database of reported incidents after deployment, and provide updates as needed to ensure effective mitigation measures.

Key contacts



Ryan Black
Partner
DLA Piper
ryan.black@ca.dlapiper.com
[View bio](#)



Alan Macek
Partner
DLA Piper
alan.macek@ca.dlapiper.com
[View bio](#)

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Gareth Stokes

Partner

Global Co-Chair, AI Practice

gareth.stokes@dlapiper.com

[Full bio](#)



Danny Tobey

Partner

Global Co-Chair AI and Data Analytics

danny.tobey@us.dlapiper.com

[Full bio](#)

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com