

Global AI Governance Law and Policy

📍 CANADA, EU, UK, US
AND SINGAPORE

Jurisdictions worldwide are designing and implementing AI governance laws and policies commensurate to the velocity and variety of the risks and opportunities presented by AI-powered technologies. Articles in this series, co-sponsored by OneTrust, dive into the laws, policies, and broader contextual history and developments relevant to AI governance in five jurisdictions: Singapore, Canada, the U.K., the U.S. and the EU.

The jurisdictions selected are a small but important snapshot of distinct approaches to AI governance regulation in key global markets. Each article provides a breakdown of the key sources and instruments that govern the strategic, technological and compliance landscape for AI governance in the jurisdiction through voluntary frameworks, sectoral initiatives or comprehensive legislative approaches.

The overview page for the full series can be accessed at the [IAPP Resource Center](#).

Contents

- Global AI Governance Law and Policy: Canada**4
 - History and context 4
 - Approach to regulation 6
 - Wider regulatory environment..... 9
 - Next steps 10

- Global AI Governance Law and Policy: EU**.....11
 - Regulatory approach 12
 - Wider regulatory environment..... 14
 - Next steps 17

- Global AI Governance Law and Policy: UK**18
 - History and context 18
 - Approach to regulation 19
 - Wider regulatory environment..... 20
 - Latest developments 21

- Global AI Governance Law and Policy: US**.....23
 - History and context 23
 - Approach to regulation 23
 - Congress 25
 - Self-regulation..... 25
 - Wider regulatory environment..... 25
 - International cooperation on AI..... 26
 - Latest developments 27

- Global AI Governance Law and Policy: Singapore**.....28
 - History and context 28
 - Singapore's approach to AI governance regulation 29
 - Wider regulatory environment..... 31
 - Latest developments 32

- Contact**.....34

Global AI Governance Law and Policy: Canada

By Ashley Casovan, Carole Piovesan and Michael Pascu

Despite its population of only 40 million, Canada has a track record of developing AI capabilities and talent. The country hosts numerous impactful startup accelerators, world-class researchers and universities dedicated to fostering a vibrant AI culture. Notably, it is home to several of the "godfathers of AI," including Geoffrey Hinton and Yoshua Bengio, who won the [Turing Award](#) in 2018 for their formative research on deep learning along with Yann LeCun.

In 2017, Canada became the first country to launch an AI strategy, seeking to understand the implications and opportunities these powerful technologies can have on its economy and society. A cornerstone of the [Pan-Canadian AI strategy](#) is the work led by the [Canadian Institute for Advanced Research](#). In close partnership with world-class national AI research institutes the Montreal Institute for Learning Algorithms, Vector Institute and the Alberta Machine Intelligence Institute, the vision of the AI strategy is to make Canada one of the world's most vibrant AI ecosystems.

Recognizing Canada's innovative potential, the federal government, provincial governments, civil society organizations and industry have been active in seeking to create the necessary frameworks within which innovation can flourish safely and responsibly.

History and context

The federal government sets national AI standards and policies, while provinces handle localized issues like data privacy. In 2017, the federal government launched the first phase of its [Pan-Canadian AI Strategy](#) with a CAD125 million investment focusing on three pillars:

- **Commercialization**, which involves transitioning AI research into practical applications for the private and public sectors.
- **Standards**, which focus on developing and adopting AI standards.
- **Talent and research**, which aim to foster academic research and enhance computing capacity for AI advancements.

In 2019, two years after launching phase one of its Pan-Canadian AI Strategy, Canada announced its [Digital Charter](#). This charter outlines 10 principles to guide the federal government's digital and data transformation efforts, with AI playing a crucial role.

In 2022, phase two of the strategy was implemented, adding over CAD433 million to the overall budget to be utilized over the course of 10 years. The importance of AI was underscored when [Bill C-27](#), also known as the Digital Charter Implementation Act, was introduced to Parliament that same year. The act includes three key components: privacy reform, the establishment of a Personal Information and Data Protection Tribunal, and the introduction of a comprehensive AI and Data Act.

While concerned about the domestic implications of AI, the country also played a significant role in turning international attention and activity toward collectively working to develop AI in a responsible manner grounded in human rights. As such, Canada, along with France, was an initial driving force behind the [Global Partnership on AI](#), a multistakeholder forum with 29 participating member nations.

Understanding the importance of leading by example, it was the first country in the world to create any AI-specific legally binding instrument. With a focus on the government's use of AI, the [Directive on Automated Decision-Making](#) was launched in 2019. Designed as a risk-based policy now popularized by the likes of the [EU AI Act](#), the DADM requires the use of a standardized [algorithmic impact assessment tool](#) to determine the risk of the

system, allowing for better alignment of risk-appropriate obligations. Many of the concepts and key requirements of this policy are similar to those in related policies published today. Making the distinction between automated decision-making versus other types of AI, additional questions about the other policies may be useful. In 2023, with the same public sector scope, the government released [guidelines](#) for generative AI.

Recognizing the need to continue to build on this policy suite in light of the ever-changing nature of AI technologies, the federal government hosted a [roundtable](#) to develop an AI strategy for the public service. This strategy focuses on three main areas: building an AI-ready workforce and fostering AI growth through innovation, enabling infrastructure and engagement, and implementing tools for responsible and effective AI adoption.

While focusing on government use of AI, in 2023 the country brought together key industry actors to commit to a voluntary [code of conduct](#) for the safe and responsible use of generative AI. These concepts are aligned with similar international efforts like the [Bletchley Declaration](#), a key agreement completed during the first [AI Safety Summit](#) hosted by the U.K.

To complement the existing efforts of the Pan-Canadian AI Strategy, the 2024 federal [budget](#) allocated CAD2.4 billion to advance AI with an eye on both internal use and external oversight. Of the budget, CAD2 billion is dedicated to a new AI Compute Access Fund as well as funding for a safety institute and advancement of sectoral research. This fund aims to invest in Canadian-made computing infrastructure to support AI businesses and researchers.

Approach to regulation

Canada is following the growing trend of regulating AI based on risk, similar to the EU AI Act. In 2022, the federal government introduced [Bill C-27](#). Part III of this bill, the [AI and Data Act](#), would establish a risk-based framework for regulating AI systems. Numerous amendments were proposed by late 2023 and are still under discussion. Below is a summary of the key concepts incorporated into the AIDA.

Similar to the EU, Canada's [approach](#) to legislating AI seeks to balance protecting rights with fostering innovation. The AIDA aims to regulate trade "by establishing common requirements, applicable across Canada, for the design, development, and use of (AI) systems" and to avoid harm by prohibiting certain conduct in relation to AI systems with a specific focus on "high-impact systems."

The AIDA proposes the following approach:

1. Building on existing consumer protection and human rights laws, the AIDA would ensure high-impact AI systems meet established safety standards. Regulations defining high-impact AI systems and their requirements are to be developed with input from a broad range of stakeholders including the industry and public to avoid overburdening the country's AI ecosystem.
2. The Minister of Innovation, Science and Industry would be empowered to administer and enforce the act, ensuring policy and enforcement evolve with technology. A new AI and Data Commissioner would be established as a center of expertise to support regulatory development and administration of the act.
3. New criminal law provisions would prohibit reckless and malicious uses of AI that would cause serious harms to Canadians.

At this time the AIDA does not ban certain AI uses outright, as the EU AI Act does. Instead, it classifies AI systems into high-impact categories, imposing stricter risk management, transparency obligations and accountability frameworks for those who make such systems available.

High-impact AI systems

The AIDA defines several high-impact uses of AI systems that carry significant responsibilities for both providers and deployers of these systems. These [use cases](#) include:

- **Employment:** AI systems used for critical employment determinations such as recruitment, hiring, remuneration, promotion and termination.
- **Service provision:** AI systems that decide whether to provide services to individuals, what type or cost of services to offer, and how these services should be prioritized.
- **Biometric processing:** AI systems that process biometric information without an individual's consent or use biometric information to assess an individual's behaviour.
- **Content moderation or prioritization:** AI systems used to moderate content on online communications platforms or prioritize the presentation of such content.

- **Health care:** AI systems used in health care delivery or emergency services.
- **Justice:** AI systems used by a court or administrative body in making determinations about individuals who are parties to proceedings before the court or administrative body.
- **Law enforcement:** AI systems used to assist a peace officer, as defined under Canada's Criminal Code, in the exercise and performance of their law enforcement duties.

including records related to data and processes used in developing the AI system.

Additional requirements also apply to AI systems that rely on machine-learning models and those making changes to high-impact AI systems.

Establishing requirements for those operating high-impact AI systems

For those managing the operations of high-impact AI systems, requirements include:

Establishing requirements for providers of high-impact AI systems

The AIDA also establishes various requirements for high-impact AI systems before they can be used in international or interprovincial trade and commerce for the first time, including:

- Assessing potential adverse impacts from intended or foreseeable uses of the system.
- Implementing measures to assess and mitigate risks of harm or biased output.
- Testing the effectiveness of these mitigation measures.
- Including features that allow human oversight of the system's operations as outlined in the regulations.
- Ensuring the system performs reliably and as intended.
- Keeping specific records demonstrating compliance with these requirements,

- Establishing measures to identify, assess and mitigate risks of harm or biased output.
- Testing the effectiveness of these mitigation measures.
- Ensuring human oversight of the system's operations.
- Allowing users to provide feedback on the system's performance.
- Keeping logs and records of the AI system's operations.
- Ceasing operations if there are reasonable grounds to suspect the system has caused serious harm or the mitigation measures are ineffective and notifying the AI and Data Commissioner.

General-purpose AI systems

The AIDA also establishes additional requirements for a general-purpose AI system, which is defined as "an artificial intelligence system that is designed for use, or that is designed to be adapted for use, in many fields and for many purposes and activities, including

fields, purposes, and activities not contemplated during the system's development." These additional requirements, which must be met by those making these systems available, include:

- Meeting certain requirements with respect to the data used to develop the system.
- Assessing potential adverse impacts from intended or foreseeable uses of the system.
- Implementing measures to assess and mitigate risks of harm or biased output.
- Testing the effectiveness of these mitigation measures.
- Including features that allow human oversight of the system's operations as outlined in the regulations.
- Including plain-language descriptions for the systems capabilities, the risks of harm or biased output, and any other information prescribed by regulation.
- If the system generates digital output consisting of text, images or audio, ensuring best efforts have been made so members of the public can identify the output as being generated by an AI system.
- Keeping records that demonstrate requirements have been met and records related to the data and processes used to develop the general-purpose system and assess its limitations and capabilities.
- Confirming an assessment has been carried out by a third-party to ensure

compliance with the requirements outlined in the regulations.

In addition to federal legislative efforts, industry-specific regulators are also updating their guidelines and requirements. For instance, the Office of the Superintendent of Financial Institutions has released a [draft guideline](#) on model risk management. Currently under consultation and expected to take effect 1 July 2025, these new guidelines will establish practices and expectations for managing the risk of models used by financial institutions, which now include AI and machine-learning methods.

To support these sectoral regulations, Canada is investing significant efforts in both domestic and international standards development for AI. As seen through the establishment of an [AI and Data Standardization Collaborative](#), the federal government recognizes the role standards will play in establishing global norms and common best practices for the appropriate development and use of AI. Through the national standards body the Standards Council of Canada, the federal government has played a significant role in the International Organization for Standardization's developments for AI. Specifically, it was one of the initial drafters of the ISO/IEC 42001 standard.

Other guidance in AI and automated decision-making includes Health Canada's [guidance document](#) on using software as a medical device, the federal government's [Guide on the use of generative AI](#) for government institutions and the Office of the Privacy Commissioner of Canada's [Principles for responsible, trustworthy, and privacy-protective generative AI technologies](#).

Wider regulatory environment

There are numerous enacted laws of relevance and application to various elements of the AI governance life cycle. The [Personal Information Protection and Electronic Documents Act](#) sets out important rules for how businesses use personal information. To modernize this law for the digital economy, the [Consumer Privacy Protection Act](#) was proposed as part of Bill C-27. The government is also working to ensure laws governing marketplace activities stay current.

Data privacy and protection

The Digital Charter Implementation Act introduces the AIDA and overhauls the PIPEDA through the Consumer Privacy Protection Act.

Combining privacy and AI regulation makes sense because data is the key link between them. The CPPA requires organizations to explain any prediction, recommendation or decision made by an automated system that significantly impacts individuals. This explanation must include the type of personal information used.

The CPPA also includes exceptions to consent for legitimate interest. However, it is unclear if this extends to using data to train AI systems. Under this exception, organizations must identify and take reasonable measures to minimize adverse effects from using data for this purpose.

Copyright and intellectual property

The AIDA does not currently address copyright issues. Instead, it appears the government aims to tackle AI and intellectual property issues through an updated Copyright Act. In 2021, before the launch of many generative AI tools, Canada began consulting on [Copyright](#)

[Act](#) updates. With rapid advancements in AI, especially generative AI, another [public consultation](#) began in December 2023.

The federal government aims to adapt the current copyright regime to address challenges posed by generative AI systems, which can produce creative content mimicking that created by humans. This raises concerns about the uncompensated use of protected works in training these AI systems, attribution and remuneration for AI-generated content, and enforcing the rights of copyright holders. Key discussion points of this consultation included text and data mining, authorship and ownership, and liability.

Consumer protection and human rights

Given the risks to human rights, including discrimination, federal, provincial and territorial human rights laws play a crucial role in protecting individuals from AI-related harms. Redress and contestability mechanisms for discrimination, like those featured in [Quebec's Law 25](#), are important, but individuals affected by AI discrimination may be unaware it has occurred. In 2021, the Law Commission of Ontario, the Ontario Human Rights Commission and the Canadian Human Rights Commission launched a joint research and policy [initiative](#) to examine human rights issues in AI development, use and governance.

Regarding consumer protections, the [Canada Consumer Product Safety Act](#) and various provincial consumer protection laws address issues like misrepresentation and undue pressure while remaining technology neutral. Updates to Ontario's consumer protection legislation, [Bill 142](#), provide insight into

potential future changes. This bill maintains a technology-neutral approach but incorporates updates reflecting the current digital landscape. Key proposed changes include new provisions on automatic subscription renewals, unilateral contract amendments and easier mechanisms for consumers to unsubscribe from services. These amendments aim to enhance transparency and fairness in consumer transactions, especially those occurring online or through automated means.

Competition

The Competition Bureau of Canada is actively engaged in the discussion around the intersection of AI and competition. In May 2024, it published a [discussion paper](#) setting out considerations for how AI may affect competition. Key topics analyzed as a part of the paper include barriers to entry, product differentiation and market power, economies of scope and scale, network effects and competitive conduct, and consumer protection.

Additionally, several other frameworks apply to AI use, including:

- [The Canada Consumer Product Safety Act](#)
- [The Food and Drugs Act](#)
- [The Motor Vehicle Safety Act](#)
- [The Bank Act](#)
- [The Canadian Human Rights Act](#), and other provincial and territorial human rights laws
- [The Criminal Code](#)

Next steps

The AIDA aims to proactively identify and mitigate risks to prevent harms from AI systems. As AI technology evolves, new capabilities and uses will emerge, requiring a flexible approach. As of June 2024, the AIDA has passed the second reading in the House of Commons, with one more reading pending, followed by three readings in the Senate.

Despite extensive proposed amendments and calls to separate the AIDA from the CPPA and the PIPEDA, it is seen by many as a significant step toward providing certainty for AI development and implementation. With a clear federal strategy in place, supported by some mandatory and many voluntary guidelines, reaching consensus on key aspects of AI governance looks to be in reach for Canada. However, even if the AIDA was to pass today, there would be a lengthy implementation timeline, likely venturing into late 2025 at the earliest.

Special thank you to Kathrin Gardhouse for her contribution to the development of this article.

Global AI Governance Law and Policy: EU

By Vincenzo Tiani, Joe Jones and Isabelle Roccia, CIPP/E

The EU has been regulating the digital sphere since the early 2000s through legislation on fundamental and other rights such as data protection and intellectual property; infrastructure through security, public procurement and resilience; technology and software such as RFID, cloud computing and cybersecurity; and data-focused legislation, including data access, data sharing and data governance. The European Commission "is determined to make this Europe's ['Digital Decade'](#)," with regulation a core component to that ambition.

In 2018, the European Commission set out its vision for AI around three pillars: investment, socioeconomic changes and an appropriate ethical and legal framework to strengthen European values. The Commission established a [High-Level Expert Group on AI](#) of 51 members from civil society, industry and academia to provide advice on its AI strategy.

In April 2019, the HLEG published its [ethics guidelines](#) for trustworthy AI, which put forward a human-centric approach on AI and identified seven key requirements that AI systems should meet to be considered trustworthy.

When European Commission President Ursula von der Leyen took office in December 2019, she pledged to "put forward legislation for a coordinated European approach on the human and ethical implications of Artificial

Intelligence" in her first 100 days. In [press remarks](#) from February 2020, she mentioned AI's potential to improve Europeans' daily lives and its role in reaching Europe's climate neutrality goals by 2050. She also set a clear objective of attracting more than 20 billion euros per year for the next decade to defend Europe's position on AI.

That announcement coincided with a Commission [white paper](#) that set out the policy options for achieving an approach that promotes the uptake of AI while also addressing the risks associated with certain uses of AI.

The [AI Act](#), first proposed by the European Commission in April 2021, was then drafted, negotiated and amended fiercely by the Commission, Parliament and Council. The agreed text will soon enter into force, combining a human-centric philosophy with

a product safety approach. The AI Act will be a keystone regulation for the development and deployment of AI in the EU and around the world. The requirements set forth in the act, combined with those that will follow from further guidance and implementation, plus the complex intersections of the act itself with the EU's broader digital governance regulatory framework, make for a deep, dynamic and exacting regulatory ecosystem for AI governance in the EU.

Regulatory approach

The AI Act is a regulation, meaning it is directly applicable in all EU member states, that seeks to guarantee and harmonize rules on AI. Compared to the EU General Data Protection Regulation, which was created to protect individuals' privacy and data protection rights, the initial proposal for an AI Act was born in the context of product safety, focusing on ensuring AI products and services on the EU market are safe. This manifested in proposed principles and requirements that are well established in the product safety context, such as technical specifications, market monitoring and conformity assessments. Many of the AI Act's now-final requirements that also protect individual rights originate from the European Parliament's positions and proposals during the trilogue negotiations with the European Commission and Council.

The AI Act is framed around four risk categories of AI systems. Each category prescribes various risk-based measures that relevant actors in the AI life cycle should take and implement. During the trilogue negotiations on the draft AI Act, requirements were added for general-purpose AI, effectively

making it an additional fifth category that, importantly, does not preclude the application of requirements attaching to other risk-based categories. For example, a general-purpose AI system might also fall within the category of high risk.

Prohibited AI systems

→ Prohibited AI systems include real-time remote biometric identification in public spaces by law enforcement with some exceptions: social scoring; emotion recognition in schools and workplaces; AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques; AI systems that exploit any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation; AI systems for making risk assessments of natural persons committing a crime; untargeted scraping of facial images from the internet or CCTV footage; use of biometric systems that categorize individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation.

High-risk cases

→ High-risk cases include when AI is used for remote biometric identification systems, but not real-time, which is prohibited, or for emotion recognition and biometric categorization based on sensitive or protected attributes or

characteristics. It also includes when AI is used in critical infrastructures, in the selection and evaluation of workers, in credit scoring, by law enforcement agencies, and in migration control by the judicial authorities. Annex III of the AI Act set out a list of high-risk applications. If an Annex III application does not have an impact on fundamental rights, health, safety or final decisions that would have been made by a human being, then it may not be considered high risk. These exemptions are intended for cases in which AI is used for ancillary actions or to improve the outcome of a human-made action. To be exempted from a high-risk classification, it is necessary to provide documentary evidence as to why the AI system should not be considered high risk.

- High-risk AI providers are therefore required to have a risk-management system in place during the life cycle of the AI. Risks to health, safety and fundamental rights must first be identified. For risks that cannot be eliminated, solutions will have to be provided so they can be mitigated and managed. For example, deployers will have to be informed and, where appropriate, trained in the use of the system. Particular attention will need to be paid to risks pertaining to children and vulnerable persons.
- Training data is required to be as representative as possible of those possibly affected by potentially negative consequences associated with the AI system. The use of sensitive data is only permitted when strictly necessary and when it is not possible to achieve the same

optimal results to avoid bias as would be the case if using synthetic or anonymous data. The handling of sensitive data is subject to heightened requirements such as a prohibition on transferring sensitive data to third parties and, once the purpose has been achieved, the sensitive data must be deleted.

Limited risk

- In limited-risk AI systems, providers have fewer obligations save for the requirement to be transparent by pointing out that AI has been used, as in the case of chatbots and deepfakes.

Minimal risk

- No additional measures are needed in minimal risk cases, such as spam filters.

General-purpose AI

- There is an obligation to keep records for general-purpose AI, including records on any copyrighted data used as part of the training data, but general-purpose AI will not necessarily be considered high risk unless it also falls within the relevant categories for high risk.
- General-purpose AI will be considered a systemic risk if it carries a specific risk that has a significant impact on the EU market due to its scale or actual or reasonably foreseeable adverse effects on public health, security or fundamental rights. General-purpose AI will also be considered a systemic risk if it has a computational power greater than 10^{25} floating point operations or so deemed by the EU AI Office, which will be responsible for such assessments.

→ Providers of such models will be subject to a number of additional obligations. These include conducting an assessment to identify and mitigate systemic risk, analyzing and mitigating such risks, and documenting and reporting serious incidents. These providers will also have to ensure an adequate level of cybersecurity protection regarding the model and its physical infrastructure.

The AI Office, housed within the European Commission, will supervise AI systems based on a general-purpose AI model in which the same provider provides the model and system. It will have the powers of a market surveillance authority. National authorities are responsible for the supervision and enforcement of all other AI systems. They will lay down rules on penalties and other enforcement measures, including warnings and nonmonetary measures. Penalties range from up to 7% of global annual turnover or 35 million euros for prohibited AI violations, up to 3% of global annual turnover or 15 million euros for most other violations, and up to 1% of global annual turnover or 7.5 million euros for supplying incorrect information to authorities.

National authorities will be coordinated at an EU level via the EU AI Board to ensure consistent application throughout the EU. The AI Board will advise on the implementation of the AI Act, coordinate with national authorities and issue recommendations and opinions. An advisory forum and a scientific panel of experts will assist EU bodies. Notably, a significant number of member states have not yet designated regulators as competent authorities under the

AI Act, and there is little information on how EU-level coordination will work in practice.

Wider regulatory environment

Recital 10 of the AI Act recalls how the AI Act "does not seek to affect the application of" the EU GDPR and the ePrivacy Directive, including the tasks and powers of the relevant authorities tasked with overseeing and enforcing those laws.

AI systems will remain subject to the GDPR to the extent they process personal data. No exception to the six legal bases for processing personal data under GDPR Article 6 has been introduced for the processing of data for AI training purposes. Pending guidelines from the EDPB to this effect, the GDPR legal bases are to be applied as before. The same applies to GDPR principles such as data minimization, privacy by design and privacy by default, which will likely conflict with organizations' business and regulatory needs to use large datasets for AI training. The interplay between GDPR principles and the AI Act in practice will undoubtedly give rise to frictions, though their scope and depth have yet to be worked through.

Article 22 of the GDPR, which grants data subjects the right not to be subject to decisions based solely on automated processing that have significant consequences, is complemented by Article 86 of the AI Act, which affords individuals the right to explanations of individual decision-making.

The member state data protection authorities remain the enforcement authorities for the GDPR when it comes to protecting personal

data used in the context of AI, even if they are not designated as the competent authorities under the AI Act. For European institutions, the competent authority is the European Data Protection Supervisor. In recent years, from the use of biometric recognition for surveillance purposes to recent developments in the field of large language models, DPAs have been active in raising the security level of these systems or banning them when the risks to fundamental rights were too high.

Article 27 of the AI Act, introduced by European Parliament, requires the completion of a fundamental rights impact assessment for high-risk AI used by public entities or private entities providing public services, such as banks and insurance companies. If, for these deployers, a data protection impact assessment already exists under the GDPR, the DPIA will be an integral part of the FRIA.

Copyright

The issue of copyright was briefly mentioned in the initial proposal of the AI Act, but following the emergence of new general-purpose AI applications on the market, rights holders demanded and obtained amendments intended to protect them.

Article 53 of the AI Act contains an explicit reference to Article 4(3) of the EU Copyright Directive 2019/790, which provides for the possibility of extracting data from databases to which one has legitimate access for data mining purposes. The article, which only concerns private entities, stipulates that rights holders may opt out of having their data mined. Therefore, if the rights holder objected, the provider would have to obtain

that right by means of a license. There are no limits, however, when data mining is done by research organizations, according to Article 3 of the directive.

The AI Act also requires organizations to provide a detailed summary of the content used in their dataset to train AI for transparency purposes. To facilitate this, the AI Office will provide a form that allows providers to present this information uniformly. This is intended to assist rights holders in verifying that their works have not been used illegitimately.

Digital Services Act

For a period during the draft AI Act trilogue negotiations, social media recommendation systems qualified as high-risk AI applications although that was later removed. However, social media and platforms producing synthetic content with AI will have to be watermarked. Digital Services Act Article 35 notes the application of watermarks could also be recommended for AI-generated content created outside the platform and uploaded to it afterward to prevent cases of systemic risk, especially in view of election periods.

Product Liability Directive

The AI Act does not regulate liability for damages resulting from AI, only the violation of the regulation's provisions concerning the safety of products and services offered, with administrative enforcement issued by national authorities.

On 14 Dec. 2023, the EU legislative institutions reached a provisional agreement on the Product Liability Directive, updating the EU's 40-year-old regulatory framework with

several important proposals relevant for AI governance, including:

- Expanding the definition of "product" to encompass digital manufacturing files and software. However, free and open-source software developed or supplied outside commercial activities falls outside the directive's scope.
- Broadening the definition of damage to include medically recognized harm to psychological health, along with the destruction or irreversible corruption of data.
- Extending the right to claim compensation to cover nonmaterial losses resulting from the damage.
- Easing the burden of proof, which remains on the injured party.
- Extending the liability period to 25 years in exceptional cases when symptoms take time to manifest.
- Introducing a cascade of attributable liability for economic operators.

The Product Liability Directive outlines various scenarios where a product is presumed to be defective or when a causal link between a defect and damage is presumed to exist.

AI Liability Directive

The proposal for a new Product Liability Directive was published with a specific proposal on AI liability. However, unlike

the Product Liability Directive, no political agreement was finalized on the AI Liability Directive before to European elections in June 2024. It remains to be seen whether the AI Liability Directive will continue in its legislative procedure, be rewritten or be abandoned during the forthcoming the 2024-29 mandate.

The EU Platform Workers Directive

According to the new Platform Workers Directive, platform workers are protected from dismissal solely based on decisions made by algorithms or automated systems. Human oversight is mandated for any decisions that impact the working conditions of individuals.

Platforms are prohibited from processing specific personal data of their workers, such as private communications with colleagues or personal beliefs. Additionally, platforms must inform workers about the utilization of algorithms and automated systems in various aspects including recruitment, working conditions and earnings.

Use of data

Concerning the use of data for training purposes, companies will need to consult recent regulations that facilitate the circulation, transfer and portability of data, including personal data with due safeguards from the Data Governance Act, the Data Act and the European Health Data Space.

Cybersecurity

The European Union Agency for Cybersecurity is working on [guidelines](#) for emerging technologies.

Next steps

The AI Act will enter into force 20 days after its publication in the Official Journal of the EU. That signals the starting point for its [phased approach](#) to implementation and enforcement, with some of the nearest term obligations, such as prohibited uses, applying by six months. The issuance of further guidance, rulemaking and enforcement by appropriate national and pan-EU regulators and bodies will add more clarifying or complexifying depth to the field of AI governance in the EU. Beyond the AI Act, many expect the next European Commission to continue or initiate regulatory work that seeks to address the tensions between AI and intellectual property, as well as the issue of AI in the workplace, AI in health and life sciences, and AI liability.

This will unfold as implementation and enforcement of the data strategy initiatives — the Data Services Act, Digital Markets Act, Data Act, Data Governance Act and data spaces like the European Health Data Space — hit full throttle, adding to the GDPR, intellectual property and product liability rules to name a few. The complexity is already crystallizing in litigation and enforcement. Many European DPAs are claiming the AI space and so are other competition and sectoral regulators. Organizations will have to factor in this intricate web of requirements and supervision as they build their AI governance programs, while also serving their business objectives.

Regardless of election results, the incoming EU leadership will likely continue to promote the EU model on the global stage, further projecting the "Brussels effect" of digital regulation.

Global AI Governance Law and Policy: UK

By Joe Jones and Michael Brown

Though the U.K. does not have any regulations specific to the governance of AI, it does have an AI Safety Institute and a variety of relevant principles-based soft law and policy initiatives, as well as binding regulation in other domains like data protection and online safety. Moreover, the development, integration and responsible governance of AI is a strategic priority across U.K. policymaking and regulatory capacity building.

History and context

The U.K. has long played an important role in the development of AI. British mathematician Ada Lovelace and computer scientist Alan Turing, the "father of theoretical computing," are widely regarded as inspiring much of the development of AI. In the 1950s and '60s, the potential of AI-generated enthusiasm and expectation led to the formation of several major AI research centers in the U.K. at the universities of Edinburgh, Sussex, Essex and Cambridge. Even today, the U.K. is regarded as a center of expertise and excellence regarding AI research and innovation.

Fast forward to September 2021, when the U.K. government's [National AI Strategy](#) announced a 10-year plan "to make Britain a global AI superpower." That plan set the stage for ongoing consideration as to whether and how to regulate AI, noting, with emphasis, AI is not currently unregulated by virtue of other applicable laws. Since 2018, the prevailing [view](#)

in U.K. law and policymaking circles has been that "blanket AI-specific regulation, at this stage, would be inappropriate" and "existing sector-specific regulators are best placed to consider the impact on their sector of any subsequent regulation which may be needed."

A consequence of the U.K. leaving the EU is that the EU AI Act — soon to enter into force — does not directly apply in the U.K. as it does to the remaining 27 EU member states. Indeed, the EU AI Act has accelerated and amplified independent U.K. policy development on whether, how and why AI should or could be regulated further and in ways more targeted than what exists via the application of existing laws to AI.

Tortoise Media's June 2023 [Global AI Index](#), which benchmarks nations on their level of investment, innovation and implementation of AI, ranked

the U.K. in fourth place, below the U.S., China and Singapore. In 2022, the U.K. ranked third. Tortoise Media commented the U.K. has an "edge in research and commercial investment."

Approach to regulation

As general context, there is no draft or current U.K. legislation that specifically governs AI. Instead, the U.K. government has focused its efforts on soft law initiatives, e.g., cross-sector regulatory guidelines, to adopt an incremental, pro-innovation approach to AI regulation.

White paper on AI regulation and consultation response

In March 2023, the U.K. government published its white paper [A Pro-Innovation Approach to AI Regulation](#) for consultation, setting out policy proposals regarding future regulation.

Notably, the document does not define AI or an AI system but explains the concepts are characterized by adaptivity and autonomy. It goes on to describe that the U.K.'s AI regulatory framework should be based on the following five cross-sectoral nonbinding principles: safety, security and robustness; appropriate transparency and explainability; fairness; accountability; and contestability and redress. Finally, the white paper does not propose the creation of a new AI regulator, instead it advocates for the empowerment of existing regulators.

In February 2024, the U.K. government published its [response](#) to the white paper's consultation, which largely reaffirmed its prior proposals with one important caveat. The response indicated future legislation is likely to "address potential AI-related harms, ensure public safety, and let us realize the transformative opportunities that the

technology offers." However, the government will only legislate when it is "confident that it is the right thing to do."

UK regulator guidelines

- Data protection: In March 2023, the U.K. Information Commissioner's Office updated its [Guidance on AI and Data Protection](#). In January 2024, it also launched a [Consultation Series on Generative AI and Data Protection](#), which is scheduled to close 12 April.
- Competition and markets: In September 2023, the Competition and Markets Authority released its [Initial Report on AI Foundation Models](#).
- Medicines and health care: In October 2023, the Medicines and Healthcare Regulatory Agency published updated guidance on [Software and AI as a Medical Device](#).
- Other: The Office of Gas and Electricity Markets and the Civil Aviation Authority are working on AI strategies to be published later in 2024. The Health and Safety Executive, the Equality and Human Rights Commission, Office of Communications, and the Financial Conduct Authority are also anticipated to release guidelines on AI use within their respective sectors in due course.

As shown above, U.K. regulators have actively prepared or published guidelines related to their own sectors. There has also been some cross-functional work on AI issues, such as with the [Digital Regulation Cooperation Forum](#), which consists of the ICO, CMA, Ofcom and FCA and is responsible for ensuring greater regulatory cooperation on online issues.

Other UK AI governmental/parliamentary initiatives

As exemplified by the following two initiatives, the U.K. government has honed its policy focus on AI safety.

- First, it organized the first-ever International AI Safety Summit in November 2023 at Bletchley Park, gathering representatives from industry, policy, academia and civil society. The summit resulted in the Bletchley Declaration on fostering international collaboration on safe frontier AI development, which was signed by representatives from over 25 territories including, China, the EU, U.K. and U.S.
- Second, it set up an AI Safety Institute staffed mostly by technical experts with the mission of minimizing "surprise to the UK and humanity from rapid and unexpected advances in AI." The institute intends to achieve this "by developing the sociotechnical infrastructure needed to understand the risks of advanced AI and enable its governance."

Separately, in November 2023, Conservative Peer Lord Holmes of Richmond introduced a Private Members' Bill, the Artificial Intelligence (Regulation) Bill. This compact document advocates for the formation of a standalone AI regulator and the new role of an AI officer for organizations that develop, deploy or use AI.

Crucially, it is rare for Private Members' Bills to be passed into law. Therefore, they are often intended to provide constructive policy recommendations or apply legislative pressure.

Wider regulatory environment

While the U.K. does not have legislation specifically governing AI, various broader statutes and case laws apply to the area. Some of the most impactful are highlighted in this section.

Data protection

From a data protection perspective, the U.K. legal system comprises the [U.K. General Data Protection Regulation](#), the [Data Protection Act 2018](#) and the [Privacy and Electronic Communications \(EC Directive\) Regulations 2003 \(SI 2003/2426\)](#). There is also, of course, proposed reform via the [Data Protection and Digital Information Bill](#), which is still in draft form and pending legislative negotiations. In addition, the [EU GDPR](#) has extra-territorial effect and likely applies to U.K. entities that process personal data relating to EU individuals.

The use of AI systems raises many compliance questions under U.K. data protection law, from establishing the roles of the data processing entities to ensuring the accuracy of personal data inputs and outputs to adhering to profiling and automated decision-making requirements.

Intellectual property

In terms of intellectual property rights, the main types in the U.K. are registered and unregistered trademarks, patents, registered and unregistered designs, copyright, and trade secrets. The key U.K. IP statutes are the [Patents Act 1977](#), [Copyright, Designs and Patents Act 1988](#), and [Trade Marks Act 1994](#).

Copyright questions are relevant to AI, given the training data may include copyright works, e.g., books, news, academic articles, web pages, photographs or paintings, and the

AI system itself may create works that could potentially be protected under copyright.

In January 2023, Getty Images commenced U.K. court proceedings against Stability AI, claiming copyright infringement. Getty alleged Stability AI "scraped" millions of images from its websites without consent and used them unlawfully to train and develop its deep-learning AI model, thereby infringing Getty's copyright works.

Patent questions are also very relevant in this area, including whether an AI system can be considered an "inventor" for the purposes of the Patents Act 1977. In December 2023, the U.K. Supreme Court dismissed an [appeal](#) from Stephen Thaler, affirming the Comptroller-General of Patents, Designs and Trademarks' decision that a machine, which embodies an AI system, could not be an inventor under the law.

Online safety

In October 2023, the [Online Safety Act](#) entered into law. It is intended to address two fundamental issues: the tackling of illegal/harmful online content and the protection of children online. It does so by imposing obligations, known under the law as "duties of care," on a sliding scale for a broad range of online entities, e.g., social media networks, search engines, video-sharing platforms, and marketplaces or listing providers.

The OSA's substantive obligations are pending secondary legislation, consultations and regulatory codes of practice, and so are not yet in force. That said, the law imposes extensive requirements that will impact AI systems, e.g., the monitoring and takedown of AI generated content that could be illegal or harmful.

Employment

From an employment law perspective, the [Equality Act 2010](#) prohibits discrimination by employers on the basis of any protected characteristics, such as age, disability, race or sex.

Due to the nature of its training data and other factors, unless mitigation steps are taken, some AI systems have the potential to exhibit biases. The use of such systems for recruiting decisions and/or performance management could therefore raise U.K. employment law compliance considerations.

Consumer protection

In terms of consumer protection, the U.K. has a patchwork of laws including the [Consumer Rights Act 2015](#) and the [Consumer Protection from Unfair Trading Regulations 2008 \(SI 2008/1277\)](#). These interact with numerous AI use cases, e.g., the information or guidance provided by chatbots to consumers or the sales contract terms between an organization and consumer for AI-related products and services.

Product liability

From a product liability perspective, the key source of law is Part 1 of the Consumer Protection Act 1987. This implements the strict liability regime set out in the [EU Product Liability Directive](#). In addition, individuals may have rights under the common law of tort and so complex issues are likely to arise regarding duties of care and liability assessments for defective AI systems.

Latest developments

Much of the U.K.'s approach to AI regulation can be classified as "latest developments." Looking ahead, there will be a steady drumbeat of regulatory and policy action as part of the U.K. government's roadmap for implementing

its approach to AI regulation. Amid that drumbeat are the following commitments and anticipated milestones.

Spring 2024

- The U.K. government will establish a steering committee for a new central governmental function to support regulatory capabilities and coordination on AI governance. The steering committee will consist of representatives from the government and key regulators, including those that are members of the DRCF.
- The U.K. government will launch targeted consultation on a cross-economy AI risk register and regulatory framework assessment.
- The DRCF [AI and Digital Hub](#) pilot will be launched. The pilot is intended to support AI innovators with queries concerning cross-regulatory AI and digital issues. Questions will be directed to the four DRCF member regulators through a single point of access and will receive tailored responses.
- The first International Report on the Science of AI Safety will be published.
- A call for views to obtain further input on securing AI models, including a potential code of practice for cybersecurity of AI, based on [NCSC guidelines](#), will be released.

During 2024

- The U.K. government is phasing in a mandatory requirement for central government departments to use the Algorithmic Transparency Recording Standard.

By end of 2024

- The U.K. government will publish an update on the voluntary responsibilities of highly capable general purpose AI systems, relating to AI safety and responsible capability scaling policies.
- The U.K. government will launch the AI Management Essentials scheme to set a minimum good practice standard for companies selling AI products and services.

By 30 April 2025

- Key U.K. regulators will publish updates on their strategic approaches to AI.

Additionally, sharpened regulatory oversight and perhaps even enforcement related to AI governance are likely to shape the U.K. AI governance ecosystem.

Global AI Governance Law and Policy: US

By Müge Fazlioglu, CIPP/E, CIPP/US

The U.S. lacks an omnibus federal law specifically targeted at the governance of AI. However, several executive orders to direct federal government policy and practice with respect to AI governance have been issued, catalyzing a series of agency regulations primarily related to government use of AI. Like the U.K., the U.S. established an AI Safety Institute, housed within the National Institute of Standards and Technology and aided by a [consortium](#) of over 200 AI stakeholders who support its mission. Numerous [states](#) have also proposed and, in some cases, enacted AI laws. Moreover, federal agencies, including the Federal Trade Commission, have made it clear their existing [legal authorities](#) apply to the use of new technologies, including AI.

History and context

The formal inception of AI as a field of academic research can be traced to Dartmouth College in Hanover, New Hampshire. In 1956, a group of scientists and mathematicians gathered for a summer workshop to test the idea that "every aspect of learning or any other feature of intelligence can be so precisely described that a machine can be made to simulate it."

Several broad strategic drivers guide the U.S.'s approach to regulating AI at a national level. These include ensuring openness and competitiveness in the AI-driven economy, improving safety while mitigating risks and the proliferation of harm, and maintaining a competitive technological edge over China.

Tortoise Media's June 2023 Global AI Index ranked the U.S. first in the world for its implementation, innovation and investment in AI. Yet, its technology-related laws and policies lag. Indeed, Tortoise ranked the U.S.'s government strategy on AI at number eight. Now, U.S. lawmakers are working to craft legislative and regulatory regimes around emerging AI technologies in ways that maximize economic benefits while managing and mitigating the risks of harm.

Approach to regulation

The U.S.'s approach to regulating AI has consisted of two primary thrusts: the promulgation of guidelines and standards through federal agencies and industry self-regulation.

National AI Research and Development Strategic Plan

A key federal policy document is the [National AI Research and Development Strategic Plan](#), which direct federal investments in AI-related research and development. First developed in 2016 and most recently updated in May 2023, this report by the National Science and Technology Council outlines a set of strategies to direct federal funding over the long- and short-term. Its goals and priorities include promoting responsible, safe and secure AI systems; fostering a better understanding of AI workforce needs; expanding public-private partnerships; and promoting international collaboration in AI.

Blueprint for an AI Bill of Rights

Issued in January 2021, the [Blueprint for an AI Bill of Rights](#) marked the Biden-Harris administration's first foray into setting the direction of national AI policy. Rather than a law or regulation imposing specific legal obligations, the blueprint is a "national values statement and toolkit." Namely, it articulates five principles to guide the design and deployment of automated systems: safe and effective systems; algorithmic discrimination protections; data privacy; notice and explanation; and human alternatives, consideration and fallback. While it did not establish any formal rules for AI systems, the blueprint served as a basis for further discussion of U.S. AI policy at the federal level.

Executive Order 14110

The next executive order on AI from the Biden-Harris administration was released October 2023. The [Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI](#), Executive Order 14110, required over

150 actions to be taken by dozens of federal agencies. Building upon the five principles of the blueprint, Executive Order 14110 added promoting innovation and competition, supporting workers, advancing federal government use of AI, and strengthening American leadership abroad. In terms of its [operational impact](#), the order directly applied to most federal agencies and those within the AI value chain that do business with the federal government.

Other federal agency guidelines

As mentioned above, Executive Order 14110 set numerous implementation milestones for federal agencies to achieve. A sample of how those and related initiatives have been enacted are listed below:

- The NIST [AI Safety Institute](#): Created as a companion resource to the AI Risk Management Framework in the wake of Executive Order 14110, the AI Safety Institute focuses on generative AI, authenticating and watermarking AI-generated content, and creating guidance and benchmarks for evaluating AI capabilities.
- The Department of State's [Enterprise AI Strategy](#) established department-wide guidance for "the responsible and ethical design, development, acquisition and appropriate application of AI." The strategy lays out a series of measurable goals around how the department will leverage and integrate AI into its mission.
- Based on the Department of Homeland Security's [AI Roadmap](#), its AI Safety and Security Board was established to issue

recommendations and best practices for critical infrastructure owners and operators to improve the security, resilience and incident response of AI systems.

Congress

While the U.S. lacks a comprehensive law designed to regulate AI governance, Congress has not been inactive on the AI front. Several bills, including the [AI Training Act](#), the [National AI Initiative Act of 2020](#) and the [AI in Government Act of 2020](#), have been enacted. While these pieces of federal AI legislation have often been lesser components of larger appropriations bills, their scopes have mirrored executive branch actions and aimed to facilitate AI adoption within the federal government and achieve coordination among federal agencies with respect to their use of AI.

Through the Senate's [AI Insight Forum](#) and bipartisan [framework on AI legislation](#), and the House of Representative's bipartisan [Task Force on AI](#), members of Congress have continued to explore how the legislature should address the promises and challenges of AI. The proposals have ranged from establishing a licensing regime administered by an independent oversight body to holding AI companies liable for privacy and civil rights harms via enforcement and private rights of action to requiring AI developers to disclose information about the training data, limitations, accuracy and safety of their models.

Self-regulation

In line with the U.S.'s long history of favoring a self-regulatory approach to industry, informal [commitments](#) have been a key policy pool in its regulatory approach to AI. In July 2023, for example, Amazon, Google, Meta, Microsoft

and several other AI companies convened at the White House and pledged their voluntary [commitment](#) to principles around the safety, security and trust of AI. These principles include ensuring products are safe before introducing them onto the market and prioritizing investments in cybersecurity and security-risk safeguards.

NIST's AI RMF

Perhaps the strongest example of the U.S.'s approach to AI regulation within the paradigm of industry self-regulation is the [AI Risk Management Framework](#), which was released by the NIST within the Department of Commerce in January 2023. The AI RMF aims to serve as "a resource to the organizations designing, developing, deploying or using AI systems to help manage the many risks of AI." To facilitate implementation of the AI RMF, the NIST subsequently launched the [Trustworthy and Responsible AI Resource Center](#), which provides operational resources, including a knowledge base, use cases, events and training.

NTIA's AI Accountability Policy

The National Telecommunications and Information Administration's [Artificial Intelligence Accountability Policy](#) also falls into the self-regulation category. The report provides guidance and recommendations for AI developers and deployers to establish, enhance and use accountability inputs to provide assurance to external stakeholders.

Wider regulatory environment

Given that AI [use cases](#) span the gamut of activity across federal agencies, oversight and collaboration have been coordinated through the [National AI Initiative Office](#), which was launched by the passage of the National AI Act of 2020. The

[National AI Advisory Committee](#) is tasked with advising the National AI Initiative Office and the president on AI-related topics.

Intellectual property

In the realm of intellectual property, efforts undertaken by the [U.S. Patent and Trademark Office](#) have centered on incentivizing innovation and inclusivity within AI and emerging technologies. The [AI/ET Partnership](#) program brings the USPTO together with the AI/ET communities from academia, industry, government and civil society. The partnership hosts listening sessions and provides public symposia and guidance at the intersection of AI and IP.

The thorny copyright law and policy issues raised by AI have been on the radar of the [U.S. Copyright Office](#) for several years. Within its AI initiative, launched in 2023, the office has held numerous public listening sessions and webinars. It also issued a notice of inquiry on copyright and AI to inform its future guidance.

In an important case pending litigation regarding AI and the fair-use doctrine, The New York Times sued the face of generative AI in [NYT v. OpenAI](#). The complaint centers around OpenAI's scraping of the newspaper's articles to train its large language models and may set a new precedent at the intersection of AI and copyright.

Employment

The Equal Opportunity Employment Commission's [AI and Algorithmic Fairness Initiative](#) was launched to ensure AI, machine learning and other emerging technologies comply with federal civil rights law. Through the initiative, the EEOC provided the public

with information and guidance on the use of AI in making job decisions for people with disabilities, mitigating discrimination and bias in automated systems, and assessing the adverse impacts of the technology in employment decisions.

Consumer protection

The U.S. federal consumer protection and antitrust agency, the FTC, took a leading role in bringing [enforcement actions](#) against companies for harmful uses of AI. At the same time, it has been proactive in warning [AI companies](#) about unfair or deceptive business [practices](#), which it has a mandate prevent. In the light of "surging" [impersonation fraud](#), the FTC recently sought public comment on a supplemental notice of proposed rulemaking to prohibit the impersonation of individuals.

Alongside the FTC, numerous other federal agencies, including the Consumer Financial Protection Bureau, EEOC, Department of Health and Human Services, Department of Justice, Department of Education, DHS, and Department of Labor joined a [pledge](#) "to uphold America's commitment to core principles of fairness, equality and justice as new technologies like (AI) become more common in daily life."

International cooperation on AI

The U.S. has been involved in numerous bilateral and multilateral efforts to advance international cooperation around AI policy, including with the EU and China. The [TTC Joint Roadmap for Trustworthy AI and Risk Management](#) aims to bridge the gap between EU and U.S. risk-based approaches to AI systems. With regard to cooperation with China around AI, a November 2023 meeting between President Joe Biden and General

Secretary Xi Jinping led the two governments to announce creation of a new bilateral [channel](#) for talks on AI.

Latest developments

In the U.S., law and policy developments related to AI are in the acceleration phase. Here's a limited preview of the most recent developments and what to expect over the next six to 18 months.

In early 2024

- The White House's Office of Management and Budget released its policy on [Advancing Governance, Innovation, and Risk Management for Agency Use of AI](#) in March 2024. The policy directs federal agencies "to advance AI governance and innovation while managing risks from the use of AI in the Federal Government, particularly those affecting the rights and safety of the public."
- Also in March 2024, the U.S. Department of the Treasury released a report on [Managing AI-Specific Risks in the Financial Services Sector](#). Written under the auspices of Executive Order 14110, the report identified "significant opportunities and challenges that AI presents to the security and resiliency of the financial services sector." It also provides next steps for addressing AI-related operational risks, such as reducing the credibility gap, enhancing regulatory coordination and expanding the NIST AI RMF to include risk management related to the financial services sector.

In late 2024

- The U.S. Copyright Office plans to issue a report based on over 10,000 comments it received in response to its August 2023 notice of inquiry.

In 2025

- Within President Biden's fiscal year [2025 budget request](#), increased funding is allotted to support further implementing activities in response to Executive Order 14110. These include increased staffing or establishment of new AI offices within the Departments of Labor, Transportation and Homeland Security, as well as additional investments in the NIST AI Safety Institute and the National AI Research Resource within the National Science Foundation.

Global AI Governance Law and Policy: Singapore

By Joe Jones and Darren Grayson Chng, CIPP/A, CIPP/C, CIPP/E, CIPP/US, CIPM, CIPT, FIP

Though Singapore does not have any regulations specific to the governance of artificial intelligence, nor a dedicated agency for AI governance, it does have a variety of relevant sectoral and voluntary frameworks as well as binding regulation in other domains – such as data protection and online safety. Moreover, the development, integration and responsible governance of AI is a strategic priority across Singaporean policymaking, putting into action the country's motto: onward Singapore.

History and context

Singapore is a country located at the southern tip of the Malay Peninsula. Frequently appearing on maps as a mere red dot, its land area is smaller than New York City's, and it has few natural resources. In order to grow and thrive, Singapore has to attract investments. It has done this by offering a pro-innovation and pro-business environment, strong digital infrastructure, and a highly skilled talent pool.

Tortoise Media's June 2023 [Global AI Index](#), which benchmarks nations on their level of investment, innovation and implementation of AI, ranks Singapore at third place, below the United States and China. [Tortoise Media](#) commented that Singapore had made "huge advancements through explicit government efforts aimed at boosting AI across innovation, research, and human capital." Further growth

in AI is expected following the Singapore government's 16 Feb. [announcement](#) that it will invest over SGD1 billion over the next five years into AI compute, talent and industry development.

In 2019, the Singapore government published its first [National AI Strategy](#), outlining plans to drive AI innovation and adoption across the economy and to deliver strong social and economic impact for Singapore. An [updated strategy](#) (NAIS 2.0) was launched in December 2023 to address recent challenges and uplift Singapore's economic and social potential over the next three to five years. Both strategies were designed and overseen by the Smart Nation and Digital Government Group, which is part of the prime minister's office and is administered by the Ministry of Communications and Information.

NAIS 2.0 seeks to achieve two goals: to advance the field of AI and maximize value creation, and to empower individuals, businesses and communities to use AI with confidence, discernment and trust. It says the Singapore government will support experimentation and innovation while ensuring AI is developed and used responsibly, in line with the rule of law and existing safeguards. Under Action 13, Singapore will regularly review and adjust frameworks to reflect emerging principles, concerns and technological developments and consider updates to broader standards and laws to support effective AI use.

To achieve these goals, the Singapore government has committed to fifteen actions:

1. Anchor new AI Centres of Excellence in Singapore-based companies to conduct value creation activities across the AI stack and explore establishing sectoral AI CoEs to drive sophisticated AI value creation and usage in key sectors.
2. Strengthen Singapore's AI start-up ecosystem, including attracting AI-focused accelerator programs to spur rapid AI experimentation.
3. Accelerate public sector adoption of AI to unlock new value propositions for citizens.
4. Update national AI research and development plans to sustain leadership in select research areas, e.g., expanding international research collaboration in areas aligned with Singapore's research priorities.
5. Attract world-class AI creators to work from and with Singapore.
6. Boost the AI practitioner pool to 15,000.
7. Intensify enterprise AI adoption for industry transformation by promoting baseline digital adoption for enterprises and providing tailored support for AI-enabled business transformation.
8. Upskill the workforce through sector-specific AI training programs.
9. Establish a dedicated physical place for AI to co-locate AI creators and practitioners and to nurture the AI community in Singapore.
10. Significantly increase high-performance compute available in Singapore.
11. Build capabilities in data services and privacy-enhancing technologies.
12. Unlock government data for use cases that serve the public good.
13. Maintain a pro-innovation regulatory environment for AI while ensuring appropriate guardrails.
14. Raise the security and resilience baseline for all system owners using AI.
15. Establish Singapore as an ambitious and pragmatic international partner on AI innovation and governance.

Singapore's approach to AI governance regulation

Compared to the EU and China, Singapore has not enacted any regulations specific to the governance of AI. Nor has the country established

a dedicated agency for AI governance. It appears that Singapore has no intention of doing so in the short term, given a statement in NAIS 2.0 that the government will "establish a common platform for regulatory agencies to coordinate on AI developments in their sector and share best practices when governing AI."

Thus, Singapore appears to be taking a sectoral approach towards AI governance regulation. Those regulatory agencies that have made moves so far have all adopted a soft law approach, preferring to issue nonbinding guidelines and recommendations.

Financial services

The [Monetary Authority of Singapore](#), Singapore's central bank and integrated financial regulator, was the first sectoral regulator to take action on AI governance regulation. Together with the financial industry, MAS created a set of [principles](#) in 2018 to guide the responsible use of AI, focusing on fairness, ethics, accountability and transparency.

In 2019, MAS announced it was working with financial industry partners to create the [Veritas framework](#) to provide financial institutions with a verifiable way to incorporate the FEAT principles into their AI and data analytics-driven solutions.

The FEAT principles and Veritas are part of Singapore's National AI Strategy, designed to help build a progressive and trusted environment for AI adoption within the financial sector.

Info-communications and media sectors

The [Info-communications Media Development Authority](#) and [Personal Data Protection Commission](#) have been the most active regulators in AI governance regulation,

launching guidelines or initiatives every year since 2019. The IMDA is a statutory board that develops and regulates the info-communications and media sectors. The PDPC is Singapore's main authority in matters relating to personal data protection.

In 2019, the IMDA and the PDPC launched the first edition of the Model AI Governance Framework at the World Economic Forum Annual Meeting in Davos. The Model Framework aims to provide private sector organizations with readily implementable guidance on key ethical and governance issues when deploying AI solutions.

Just a year later, in 2020, the IMDA and PDPC updated the Model Framework, launching the second edition together with an [Implementation and Self-Assessment Guide for Organisations](#), which aims to help organizations assess the alignment of their AI governance practices with the Model Framework, and a [Compendium of Use Cases](#), which illustrates how organizations implemented accountable AI governance practices, and aligned with AI governance practices with the Model Framework.

In 2022, the IMDA launched [AI Verify](#), an AI governance testing framework and software toolkit that validates the performance of AI systems against a set of internationally recognized principles through standardized tests.

In mid-2023, Singapore's Minister for Communications and Information announced the launch of the [AI Verify Foundation](#) to support the development and use of AI Verify. At around the same time, an IMDA [director](#) said it was not looking at regulating AI then, but might introduce regulation later.

Health sector

In October 2021, the Ministry of Health published the [AI in Healthcare Guidelines](#) to support patient safety and improve trust in the use of AI in health care. These guidelines were co-developed with the Health Sciences Authority and the Integrated Health Information Systems, now known as Synapse, and complemented HSA's [regulations](#) of AI medical devices.

Wider regulatory environment

Although Singapore does not have binding regulations specific to AI, there are numerous laws of relevance and application to various elements of the AI governance lifecycle.

Data protection

The Personal Data Protection Act governs the collection, use, disclosure and care of personal data in Singapore. It provides a baseline standard of protection for personal data and complementing sector-specific regulatory provisions, such as those found in the Banking Act and Insurance Act. In 2023, the PDPC released draft advisory guidelines on the use of personal data in AI recommendation and decision systems for public consultation. The advisory guidelines provide guidance on how the PDPC will interpret the PDPA, so even though they are not legally binding, organizations view them as instruments that should be complied with. It is anticipated the finalized advisory guidelines will be issued in the first half of 2024.

Copyright

The Copyright Act protects the expression of ideas in tangible form, so long as the work is original, i.e., not copied. Similar to the U.S., and unlike the U.K., the work must also have been created by an identifiable human author. Copyright infringement occurs when

a copyright owner's rights are violated, which can occur when copyrighted work is copied, distributed, performed or displayed without the copyright owner's permission. An exception, known as "fair dealing," permits the use of nonsubstantial parts of copyrighted work for study or research. The wilful infringement of copyright is also a criminal offense if it is significant and the infringer commits the infringement to obtain a commercial advantage. Regarding AI specifically, source codes, AI algorithms, and data compilations including databases, may be protected by copyright. At this point it is unclear if the fair dealing exception can apply to the use of copyrighted works for training AI models.

Online safety

In 2022, the Online Safety (Miscellaneous Amendments) Bill was passed to enhance online safety for Singapore users. Providers of "online communication services," i.e., electronic services that allow Singapore users to access or communicate content via the internet, with significant reach or impact, must comply with the Codes of Practice issued by IMDA. So far, this new rule only covers social media services, and IMDA has issued one Code of Practice for online safety. The amendments also empower IMDA to issue directions to deal with specified "egregious content" that can be accessed by Singapore users.

The Online Criminal Harms Act, passed in 2023, enables the Singapore Government to deal more effectively with online activities that are criminal in nature.

A Centre for Advanced Technologies in Online Safety was established in April 2023 by the Agency for Science, Technology and Research

to host research on technological capabilities to combat online harm, including tools and measures to detect deepfakes and nonfactual claims, inject watermarks, trace the origin of digital content, and help vulnerable groups verify information they encounter online.

Antidiscrimination

All employers in Singapore are expected to adhere to the Tripartite Guidelines on Fair Employment Practices, which contain principles of fair employment practices, for example, that employers must recruit and select employees on the basis of merit, such as skills, experience or ability to perform the job, and regardless of age, race, gender, religion, marital status and family responsibilities, or disability.

International co-operation on AI

Under NAIS 2.0, as part of establishing Singapore as an international partner for AI innovation and governance, the Singapore government wants to continue growing its international networks with key partner countries and leading AI companies.

So far, half of Singapore's digital economy agreements contain AI modules promoting the adoption of ethical governance frameworks for AI and, where appropriate, the alignment of governance and regulatory frameworks. The intention is to align with foreign partners on a common set of AI governance and ethics principles so compliance by organizations is more easily achievable and less burdensome.

The U.S. National Institute of Standards and Technology and IMDA published a crosswalk in October 2023, mapping the NIST's AI Risk Management Framework 1.0 to AI Verify. IMDA

said this joint effort signaled both parties' common goal of balancing AI innovation and maximizing the benefits of AI technology while mitigating technology risks.

In November 2023, Singapore's prime minister participated in the AI Safety Summit organized by the U.K. at Bletchley Park. Together with 28 other economies, Singapore signed the Bletchley Declaration, agreeing to work together to prevent "catastrophic harm, either deliberate or unintentional," which may arise from AI computer models and engines.

Singapore is not a member of the Organisation for Economic Co-operation and Development but was invited to take part in its Expert Group on AI. Singapore is a founding member of the Global Partnership on AI, an international initiative to promote responsible AI use that respects human rights and democratic values.

Latest developments

In January 2024, the IMDA issued the Proposed Model AI Governance Framework for Generative AI and, launched the Generative AI Evaluation Sandbox with Enterprise Singapore, a government agency championing enterprise development, in early February.

The proposed framework was developed with the AI Verify Foundation. It "seeks to set forth a systemic and balanced approach to address generative AI concerns while continuing to facilitate innovation."

There are nine dimensions in the proposed framework that IMDA says must be looked at in totality to foster a trusted ecosystem:

1. Accountability.

2. Quality data and addressing potentially contentious training data in a pragmatic way.
3. Trusted development and deployment by enhancing transparency and disclosure.
4. An incident-management system for timely notification and remediation.
5. Third-party testing against common AI testing standards.
6. Security.
7. Transparency about where content is from.
8. Global cooperation among AI safety research and development institutes.
9. "AI for Public Good" i.e., harnessing AI to benefit the public by democratizing access, improving public sector adoption, upskilling workers and developing AI systems sustainably.

→ The development of the broader AI governance ecosystem in Singapore. The nine dimensions could just as easily apply to AI in general, raising the question of what kind of impact or relationship the proposed framework will have on future AI governance regulation.

The [Generative AI Evaluation Sandbox](#) is not directly linked to the proposed framework but is an initiative that the IMDA launched with EnterpriseSG to support companies in gaining hands-on experience with generative AI solutions. How it works: 13 generative AI solutions will be onboarded to the sandbox by the end of February 2024. Local small- and medium-sized enterprises selected to participate in the sandbox will receive grant support to trial a solution of their choice for three months. When the sandbox concludes, IMDA and EnterpriseSG will review the SMEs' feedback to evaluate the solutions and consider scaling the adoption of generative AI applications across local SMEs.

Though ostensibly targeted at generative AI, the nine dimensions in the proposed framework will be of interest to those following and tracking:

- The implementation of NAIS 2.0 regarding AI governance regulation. For instance, dimension nine adopts part of NAIS 2.0's vision to "achieve AI for the Public Good, for Singapore and the World."

Contact

Joe Jones

Director of Research and Insights, IAPP

jjones@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media



Published June 2024.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2024 IAPP.

All rights reserved.