JONES DAY | One Firm Worldwide®


# WHITE PAPER

October 2025

## Rising Global Regulation for Artificial Intelligence

Artificial intelligence ("AI") is a global subject of intense focus by governments, research institutions, investors, and corporations, ranging from start-ups to well-established industry leaders. As technology and regulatory frameworks evolve at a rapid pace, complex and novel legal issues continue to arise in transactional, litigation, and regulatory compliance contexts.

As an update to our December 2022 publication with the same title, this *White Paper* highlights key regulatory developments and questions that merit consideration by private-sector leaders and in-house counsel, in particular regarding AI risks and risk management of AI.

## INTRODUCTION

The use of AI and interest in its diverse applications are steadily increasing across a wide range of industries, including advertising, banking, telecommunications, manufacturing, retail, energy, transportation, health care, life sciences, waste management, defense, and agriculture. Businesses are turning to AI systems and the related technology of machine learning to increase their revenue, quality, and speed of production or services, or to drive down operating costs through automating and optimizing processes previously reserved to human labor. Government and industry leaders now routinely speak of the need to adopt AI, maintain a "strategic edge" in AI innovation capabilities, and ensure that AI is used in correct or humane ways. Some major jurisdictions are increasingly focusing on AI as a national security concern.

Despite these developments, many major jurisdictions, including in the United States and the United Kingdom, have not yet developed a single common body of "AI law"—or even an agreed-upon definition of what AI is or how it should be used or regulated. With applications as diverse as chatbots, facial recognition, digital assistants, intelligent robotics, autonomous vehicles, medical image analysis, and precision planting, AI resists easy definition and implicates areas of law that developed before AI became prevalent. Because it requires technical expertise to design and operate, AI can seem mysterious and beyond the grasp of ordinary people. Indeed, most lawyers or business leaders will never personally train or deploy an AI algorithm—although they are increasingly called on to negotiate AI-related issues, resolve AI-related disputes, or become well-versed in the risks and challenges that AI presents to their organizations.

This *White Paper* examines the core legal concepts that governments in several jurisdictions—the European Union, the People's Republic of China ("PRC" or "China"), the United Kingdom, Japan, Australia, and the United States—are developing in their efforts to regulate AI and encourage its responsible development and use. Although AI legal issues facing companies will often be specific to particular industries, products, transactions, and jurisdictions, this *White Paper* also includes a checklist of key considerations that in-house counsel may wish to address when advising on the risk as well as the development, use, deployment, or licensing of AI, either within a company or in the transactional context. Ultimately, governments are implementing divergent and sometimes conflicting requirements. A strategic perspective and an ability to explain technical products to regulators in clear, nontechnical terms will help companies navigate the current legal terrain.

### WHAT IS AI?

AI comprises complex mathematical processes that form the basis of algorithms and software techniques for knowledge representation, logical processes, and deduction. One core technology behind AI is machine learning, in which AI models can be trained to learn from a large amount of data to draw correlations and patterns, which enables them to be used, for example, in processing and for making autonomous decisions.

New forms of AI are emerging and evolving on a near-constant basis. For example, generative AI ("GenAI") focuses on creating new content by learning patterns from existing data, while predictive AI analyzes data to forecast outcomes and trends. Agentic AI, in contrast, is focused on decision-making and completing routine tasks with limited human intervention. When trained and applied correctly, AI can unlock tremendous gains in productivity—enabling results or insights that would otherwise require prohibitively lengthy periods of time to achieve by means of human reason alone, or by humans using traditional computing techniques.

For example, predictive AI can replace or augment "rote" tasks by analyzing historical data, identifying patterns, and automating repetitive processes to enable faster and more accurate decision-making than manual efforts. In other cases, GenAI can generate text (including computer code), sound, images, video, or other content in response to a user's prompt. Agentic AI's ability to take proactive steps in pursuit of complex objectives makes it a natural fit for decision-oriented applications, like virtual assistants, consistent with recent Organization of Economic Cooperation and Development and ISO/IEC 42001:2023 definitions that emphasize autonomy, goal-oriented behavior, and accountability. An AI tool's outputs, analysis, and recommendations may offer efficiencies to a human actor, who is able to save time and hone in faster on key issues.

## WHY REGULATE AI?

In many industries, integrating AI-based technology is considered critical to securing long-term competitiveness. Most industrial countries have already started the race for world market leadership in AI technologies through various means, such as public funding, private-sector investments, and military defense applications, which can drive further innovation. In addition, some governments seek to support AI's growth through legislative frameworks that allow the technology to develop and optimize its potential.

However, as has been widely reported, AI systems can present significant risk. For example, predictive AI can contribute to the creation of "echo chambers" that display content based only on a user's previous online behavior to "predict" what is desired or believed by that user, thereby reinforcing their views and interests or exploiting their vulnerabilities. A GenAI tool might "hallucinate" inaccurate or incomplete information in response to a user prompt, or it may lack appropriate guardrails to protect the confidentiality of inputted information. Depending on the application of the AI, a tool could pose a safety or security risk.

Governments seeking to regulate AI aim to build citizen trust in such technology while limiting potentially harmful applications. Yet governments (and different agencies within the same government) often vary on what constitutes an appropriate manner of training and using AI. What one authority sees as a feature, another may see as a bug. Further, they—and regulated publics—may disagree on the ideal relative weight to place on important considerations such as privacy, transparency, liberty, and security.

As governments apply different perspectives to this technically complex (and often inherently multijurisdictional) area, regulated parties face a complex and sometimes contradictory body of regulatory considerations that is unsettled and changing rapidly. Training, deploying, marketing, using, and licensing AI, particularly if these activities occur across multiple jurisdictions, increasingly requires a multidisciplinary and multijurisdictional legal perspective.

## HOW IS AI REGULATED?

AI's rapid expansion has led to increased legislative and regulatory initiatives worldwide. These global legal initiatives generally aim at addressing three main categories of issues:

**Data Ecosystems**. First, legislation and regulations seek to create vibrant and secure data ecosystems to foster AI development and deployment. Data is required to train and build the algorithmic models embedded in AI, as well as to apply the AI systems for their intended use.

- In the European Union, AI's demand for data is regulated in part through the well-known EU General Data Protection Regulation ("GDPR")[1]. Additionally, the EU Data Act, which facilitates data access and sharing, entered into force in January 2024. The United Kingdom similarly implemented data protection measures through the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018.
- In comparison, the United States has taken a more decentralized approach to the development and regulation of AI-based technologies and the data that underpins them. Federal regulatory frameworks—often solely in the form of nonbinding guidance—have been issued on an agency-by-agency and subject-by-subject basis, and authorities have sometimes elucidated their standards only in the course of congressional hearings or agency investigations rather than through clear and prescriptive published rules.
- The People's Republic of China has implemented data-security and protection laws to prevent unauthorized data exports. Meanwhile, new administrative measures promote and regulate cross-border data flow by raising data volume thresholds and providing conditional exemptions from prerequisite procedures (e.g., security assessment, standard contracts clauses, or personal information protection certification). Free trade zones can issue and implement their own "negative lists," allowing data to be freely exported without these procedures, resulting in freer AI data flows. While the central government promulgates generally applicable laws and regulations, specialized government agencies have provided regulations specific to their respective fields, and local governments are exploring more efficient but secure ways to share or trade data in their areas, such as setting up data exchange centers.

**Market Access**. Second, regulators in multiple jurisdictions have proposed or enacted restrictions on certain AI systems or uses believed to pose safety and human-rights concerns. Targets for such restrictions include AI-powered autonomous machines capable of taking lethal action without a meaningful opportunity for human intervention, or AI social or financial creditworthiness scoring systems that pose unacceptable risks of racial or socioeconomic discrimination.

- In the European Union, the sale or use of AI applications is subject to uniform EU-wide conditions (e.g., standardization or market authorization procedures). For instance, the EU AI Act aims to prohibit market access for high-risk AI systems, such as AI systems intended for the "real-time" remote biometric identification of natural persons in publicly accessible spaces for the purposes of law enforcement, subject to applicable exemptions.
- In the United Kingdom, the government has set up the AI Safety Institute ("AISI"), which is a research organization aimed at assessing and advising policymakers on the safety of advanced AI systems. The AISI will be pivotal in advising the government on the technical aspects of implementing AI safety measures in future legislation.
- Members of Congress in the United States have advanced legislation that tackles certain aspects of AI technology, though in a more piecemeal, issue-focused fashion. For instance, recently passed legislation aims to combat the effect of certain applications of generative adversarial networks capable of producing convincing synthetic likenesses of individuals (or "deepfakes") on U.S. cybersecurity and election security. Australia has likewise passed legislation making it illegal to share sexually explicit deepfakes without consent. Japan has not yet issued mandatory laws or regulations restricting application of AI in any specific area for concerns such as discrimination or privacy.
- The PRC has swiftly reacted to AI technologies by issuing a series of new regulations that establish concrete requirements for the development and use of AI in China. National standards have also been promulgated as supporting documents for the implementation of these regulations. The PRC also regulates various aspects important to the realization and development of AI, such as ethics, data security, personal information and privacy protection, automation, and intellectual property and trade secret protection, among others.

**Liability**. Third, governments are just beginning to update traditional liability frameworks, which are not always deemed suitable to adequately deal with damages allegedly "caused by" AI systems due to the variety of actors involved in the development, interconnectivity, and complexity of such systems. Thus, new liability frameworks are under consideration, such as establishing strict liability for producers of AI systems, to facilitate consumer damage claims. The first comprehensive proposal came from the European Union's new Products Liability Directive,[2] which may apply to certain AI systems.

Each of these categories is discussed in the following sections.

## DEVELOPING A DATA ECOSYSTEM

Often depicted as the fuel of AI, data is essential to develop and deploy AI systems. AI systems are built with algorithms, which in turn require configuration and training with datasets. To achieve a thriving data ecosystem that meets AI needs depends on so-called Big Data, i.e., data that fulfills a "triple-V" criteria:

- Volume: abundant data that increases the accuracy of the analysis;
- Variety: data that is diverse in nature and from diverse sources, which the AI system can structure and correlate most efficiently; and
- Velocity: data that is up-to-date and transmitted in real-time (e.g., from sensors).

One could also add a fourth "V" of Veracity (i.e., data accuracy). All of these characteristics lead to a fifth "V" of Value: data that fulfills the above criteria presents the most value for AI systems.

Given the central role of data in AI systems, the regulation of data use and access is critical. Availability and access to extensive, quality-assured datasets are key to the configuration, training, and application of AI systems. However, regulation may impede or advance such use and access. Data sets are not always openly available, and their use can be restricted, for example, by intellectual property or privacy rights. Data ownership is also important and may be impacted by regulation seeking to lower barriers to entry and switching. Furthermore, data regulation can also address the veracity element, as datasets can be biased where implemented data is insufficiently screened and therefore not representative of a model's intended outcome, resulting in biased algorithms that may pose ethical and potentially legal concerns.

## EUROPEAN UNION

### Personal Data

The European Union has increasingly regulated the use of data, i.e., data processing. Initially, personal data was the focus of such regulation, notably starting in 2016 with the GDPR. By seeking to establish a human rights-centric approach to technology, and to provide individuals with better control over how their personal data is processed (i.e., for a legitimate purpose in a lawful, fair, and transparent way), the GDPR aims to establish a framework for digital trust, while providing for free movement of personal data within the European Union. It also regulates how international data flows outside the European Union can take place.

However, tension exists between bedrock GDPR principles (such as purpose limitation and data minimization) and the full deployment of the power of AI and Big Data.[3] For instance, AI depends on vast quantities of data processed for purposes often not fully determined at the time of collection, in arguable tension with the GDPR's purpose limitation requirement. The use of data for training or using AI also faces potential constraints under the GDPR's requirement to have a legal basis (such as individual consent) for personal data processing. For this reason, for instance, facial recognition based on online data is restricted by data protection authorities in several EU Member States.

European data protection authorities have issued an opinion on certain data protection aspects related to the processing of personal data in the context of AI models,[4] following a stakeholder event on AI models organized by the European Data Protection Board ("EDPB") in November 2024.[5] The opinion emphasizes that AI models trained with personal data cannot always be considered anonymous and need to be assessed on a case-by-case basis. It also outlines a three-step test for using legitimate interest as a legal basis for processing personal data during AI model development and deployment: identifying the legitimate interest; assessing the necessity of the personal data processing; and conducting a balancing test to ensure data subject rights under the GDPR are respected. The EDPB Guidelines 02/2025 (adopted June 20, 2025) further clarify that legitimate interest is unlikely to apply to the large-scale scraping of publicly accessible personal data for AI training.[6]

As an example of the Brussels effect, the GDPR became a model for many other laws around the world, including in Chile, Brazil, Japan, South Korea, and Argentina.

### Non-Personal Data

For non-personal data, the European Union adopted a regulation on the Free Flow of Non-Personal Data[7] in 2018 to ensure free movement of such data and prohibit Member States from adopting (restrictive) data localization laws similar to other jurisdictions. Additionally, the European Union's Open Data Directive[8] sets minimum rules allowing government-to-business ("G2B") data sharing through the publishing of data held by public authorities in dynamic and machine-readable format and through standardized application programming interfaces ("APIs").

In 2020, the European Union also announced a European Strategy for Data[9] to more broadly address all data flows and develop an EU single market for data, such that:

- Data can flow within the European Union and across sectors;
- European rules and values are fully respected, including data protection, consumer protection, and fair competition;

- Rules for access and use of data are fair, practical, and clear. This includes a clear and trustworthy data governance mechanism and an open but assertive approach to regulating international data flows; and
- Data is secure and, in the case of industrial data, easily accessible to businesses.

The EU Strategy for Data also identified issues of concern, including insufficient data availability, unequal market power, insufficient data governance, inadequate data infrastructures and technologies, and poor data interoperability and quality.

As a result, the European Union adopted a Data Governance Act ("DGA")[10] in May 2022, which aims to facilitate voluntary data sharing by individuals and businesses through enhanced trust in such sharing. The DGA promotes trusted sharing through neutral data brokers and through so-called "data altruism organizations" for gathering data voluntarily donated by individuals. The DGA further facilitates the sharing of G2B data that is subject to third-party privacy, intellectual property, or commercial confidentiality rights.

Of broader-scale impact, the European Union also adopted the Data Act[11] in December 2023, which mostly became applicable in September 2025. This regulation aims to create a fair and competitive data market by facilitating data sharing and reuse across sectors, empowering users of connected products (mainly consumers and businesses) to control and access the data they generate. It seeks to increase competition, particularly for small and medium-sized enterprises, by setting interoperability standards and preventing unfair contractual terms. It also impacts cloud service providers by requiring them to ensure data portability and interoperability, making it easier to switch between different cloud services. These data interoperability obligations now intersect with the EU AI Act's requirements for General Purpose AI ("GPAI") model providers effective August 2, 2025, particularly in ensuring transparency and dataset documentation.[12]

In parallel, the European Union has also developed and continues to promulgate sector-specific data regulations to boost the EU data economy. Existing EU law already provides for some forms of data-sharing obligations in the banking sector for payment data,[13] in the energy sector for smart meter/consumption data,[14] and data provided to or created by digital content/services (all concerning personal data),[15] as well as in the automotive sector for repair and maintenance information[16] and intelligent transport systems[17] (including potentially in-vehicle data[18] and alternative fuels infrastructure[19]) (all non-personal data). The Digital Markets Act ("DMA"),[20] adopted in March 2022 and published in October 2022, also imposes certain data access obligations on those deemed as "gatekeepers" of core platform services (e.g., obligations to make data generated by business users available to vendors using the platform or to provide access to search data to search engine competitors).

**In addition, the European Commission will pursue regulatory frameworks for the development of sectoral "data spaces" in the below 14 areas.**

### EU Data Spaces

- Industrial (manufacturing)
- Green Deal
- Mobility
- Skills
- Health
- Financial
- Energy
- Agricultural
- Public Administrations
- Cultural Heritage
- Language
- Media
- Research and Innovation
- Tourism

For the first data space to be established, the European Health Data Space ("EHDS"), the European Commission published a proposed regulation on May 3, 2022.[21] On April 24, 2024, the European Parliament formally adopted a provisional political agreement earlier reached with the Council on March 15, 2024, on the proposed regulation on the EHDS.[22] The regulation entered into force on March 26, 2025,[23] and its provisions become applicable gradually over several years, with secondary use provisions starting in 2029 and certain interoperability obligations for health data exchange applicable between 2027 and 2028.[24] The EHDS regulation aims at giving patients easy access to their health data to facilitate sharing their data with health professionals across the Member States. It also foresees specific rules on secondary use of electronic health data, e.g., for research and personalized medicine.

## TABLE 1–SUMMARY OF MAIN EU DATA ACCESS REGULATIONS AND PROPOSALS

| Name of Legislation | Type of Data | Main Purpose | Status25 |
|---|---|---|---|
| **General** | | | |
| **General Data Protection Regulation** | Personal data | Privacy protection | Applicable since May 25, 2018 |
| **Free Flow of Data Regulation** | Non-personal data | Prevent data localization laws | Applicable since May 28, 2019 |
| **Open Data Directive** | All data | G2B data sharing | Transposition by July 17, 2021 |
| **Data Governance Act** | All data | G2B data sharing | Applicable since September 24, 2023 |
| **Data Act** | All data | Control over data and ensure interoperability | Entry into force on January 11, 2024; applicable on September 12, 2025, except interoperability obligations for smart contracts, which apply from September 12, 2026 |
| **Sector-Specific** | | | |
| **Digital Markets Act** | Certain data held by "gatekeepers" | Promote fair competition | Applicable since May 2, 2023 |
| **Revised Payment Services Directive** | Payment data | Open payment services | Transposition by January 13, 2018 |
| **Electricity Directive** | Smart meter/consumption data | Energy consumption data availability | Transposition by December 31, 2020 |
| **Gas Directive** | Smart meter/consumption data | Energy consumption data availability | Entry into force on August 4, 2024; transposition by August 5, 2026 |
| **Digital Content and Services Directive** | Digital content/services data | Digital content/services | Transposition by July 1, 2021 |
| **Motor Vehicle Regulation** | Repair and maintenance data | Aftermarkets for repair | Applicable since September 1, 2020 |
| **New Intelligent Transport Systems Directive** | Intelligent transport systems data | Smart transport systems | Entry into force on December 20, 2023; transposition by December 21, 2025 |
| **Alternative Fuels Infrastructure Regulation** | Recharging infrastructure data | Interoperability of recharging infrastructure | Applicable since April 13, 2024 |
| **European Health Data Space Regulation** | Health data | Access to personal electronic health data | Entry into force on March 26, 2025; key parts applicable on March 26, 2029 |

### Regulatory Oversight of Data Ownership, Data Pooling, Data Access, and Portability

Data increases in value when available in large pools. This increase in value creates competitive incentives to collect and pool data. In turn, data pooling and aggregation create risks of lock-in effects and raising barriers to entry and switching through increased network effects, even if data is "non-rivalrous" (i.e., it can always be copied). These issues can be dealt with by EU and/or national competition law. For example, data-pooling agreements between competitors could be limited to only certain circumstances,[26] such as when established through trade associations.[27] Similarly, competition authorities could investigate practices whereby certain dominant companies refuse to provide data akin to an essential facility.[28]

EU regulation has also progressively sought to facilitate data portability and access through third parties. The GDPR already requires data portability for personal data under certain circumstances. The Free Flow of Data Regulation, concerning non-personal data, also includes rules on the porting of data for professional users via industry codes of conduct. The DMA also includes rules requiring the portability of data held by gatekeepers. It sets out data access rights for business users of gateway service providers (such as online marketplaces).

The EU Data Act now seeks to bring access and data portability to an entirely new level, as it would include access and portability rights applicable to users and third parties, in particular in the cloud sector. The EU Data Act also limits the ability to rely on database IP rights to oppose sharing.

However, imposing a data-access obligation does not necessarily mean that access should be given for free. Most legislation does not foresee any pricing mechanism, with few exceptions.[29] This regulatory gap raises the thorny issue of the appropriate level of compensation, price regulation, and the need to apply fair, reasonable, and non-discriminatory, or FRAND, conditions. Such a scenario brings heightened potential for litigation, and businesses should carefully assess related risks.

In addition to regulating the aggregation and sharing of data, the European Commission recently issued a recommendation urging Member States to start reviewing outbound investments outside of the European Union in highly strategic sectors, including AI.[30] The recommendation seeks to strengthen economic and national security interests and aligns with a U.S. rule with similar aims.[31] On January 15, 2025, the European Commission issued a nonbinding recommendation on screening outbound investments, urging Member States to review transactions involving critical technologies—artificial intelligence, semiconductors, and quantum technologies—and asked Member States to report to the Commission on their findings and risk assessments by June 30, 2026.[32]

## UNITED KINGDOM

The UK data protection regulator is the Information Commissioner's Office ("ICO"). The processing of personal data is governed in the United Kingdom by the UK GDPR (which implements similar measures to the EU GDPR) and Data Protection Act 2018 ("DPA"). Where use of AI involves the processing of personal data (which is often likely to be the case), such use is regulated by the UK GDPR and DPA. In addition, the Equality Act 2010 and administrative law are also relevant to the development and use of AI.

The ICO has issued a paper setting out its strategic approach to the regulation of AI[33] as well as a range of guidance to assist organizations in complying with data protection requirements in relation to AI.[34]

Since January 2024, the ICO launched a series of consultations on GenAI. The series comprised five parts and considered the following areas:

- An assessment of the lawful basis for web scraping to train GenAI models, noting "training generative AI models on web scraped data can be feasible if generative AI developers take their legal obligations seriously and can evidence and demonstrate this in practice";[35]
- How the purpose limitation should be applied at different stages of the GenAI life cycle;
- How the UK GDPR's accuracy principle applies to the output of GenAI models and the impact that accurate training data has on that output;
- Assessing data-subject rights in relation to the training and fine-tuning of GenAI; and

Allocating controllership across the GenAI supply chain.

### Cyber Security and Resilience Bill

In the United Kingdom, the existing cross-sector cyber regulations reflect law inherited from the European Union. The United Kingdom has now introduced the Cyber Security and Resilience Bill to cover AI and cybersecurity reforms.[36] The bill will be introduced to the UK Parliament later this year and is aimed at expanding the remit of the regulation to protect more digital services and supply chains, while also giving regulators more powers to investigate vulnerabilities in cyber-safety mechanisms.

### Data Protection and Digital Information Bill

This measure introduces a number of changes to the United Kingdom's data protection regime. These include measures to reduce transparency obligations and allow for wider use of automated decision-making, which will both have implications for the use of AI in the United Kingdom.

## UNITED STATES

### Patchwork of Competent Authorities

In the United States, administrations and members of Congress of both parties have declared AI as one of the central strategic and economic issues of the 21st century and have convened blue-ribbon panels to advise the White House, Congress, and federal agencies on AI's policy challenges and opportunities.

Compared with the response in other jurisdictions, efforts to create a substantive legal framework to regulate AI's development and use have been comparatively slow and less comprehensive. Only a handful of federal agencies have addressed specific issues posed by AI technologies in select fields. For example:

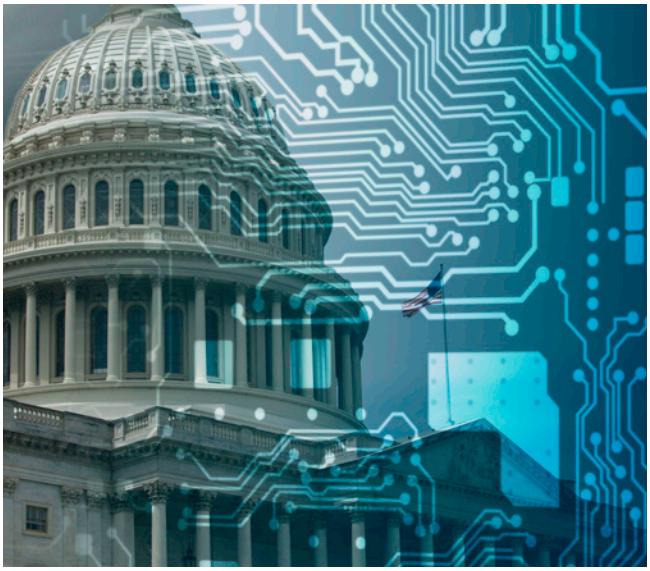
- In response to the increasing prevalence of AI-based automated vehicles, the Department of Transportation's ongoing efforts focus on enabling AI's safe integration into the transportation system and adopting and deploying AI-based tools into internal operations, research, and citizen-facing services.
- The Food and Drug Administration proposed a regulatory framework for AI-based software incorporated into medical devices.[37]
- The Department of Commerce's Bureau of Industry and Security amended its Export Administration Regulations to impose national security-based license requirements on exports or transfers of certain AI technologies, and the Committee on Foreign Investment in the United States ("CFIUS") has similarly indicated that foreign investments in "critical technology" AI companies may be subject to heightened filing obligations and a more exacting review.
- The Department of Commerce's National Institute of Standards and Technology ("NIST"), the Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau ("CFPB"), and the Federal Housing Finance Agency ("FHFA") have each promulgated guidelines aimed at addressing AI risks and protecting consumers from misuse of AI.
- Pursuant to Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," the Department of Justice ("DOJ"), Department of Homeland Security, and other federal agencies have promulgated regulations that prevent or restrict certain transactions involving sale, access, sharing, and transfer of personal data.[38]
- The Department of the Treasury established a new Outbound Investment Security Program, prohibiting investments abroad that pose an acute national security threat, including in AI.[39] Similarly, the Department of Commerce's Bureau of Industry and Security issued a rule establishing a framework to prevent U.S. adversaries from accessing the most advanced AI systems.[40]

AI-focused legislative activity has likewise been approached in a piecemeal fashion at both the federal and state levels. The majority of initiatives at the federal level have targeted specific trends in AI technologies (e.g., eliminating perceived discriminatory bias in AI-based lending technologies, combating "deepfakes") or provided funding or other government support to advance the U.S. role in developing AI technology. Importantly, however, federal initiatives generally have been limited to guidance or new proposed rules rather than final binding standards or new legislation. State legislatures have taken varied approaches when crafting AI-related laws. The majority of state laws are prohibitory in nature, seeking to regulate discriminatory uses of AI and protect consumers' data.

**Federal AI Policy.** Recent developments have significantly shifted the federal approach to AI regulation and policy. In July 2025, the White House released a comprehensive AI Action Plan and issued three major executive orders that signal a new era of federal leadership in AI governance, infrastructure, and international engagement.[41] Centered around three pillars—accelerating AI innovation, building robust AI infrastructure, and leading in international AI diplomacy and security—the plan emphasizes deregulation to foster innovation, protection of ideological neutrality in AI systems, support for open-source AI, workforce empowerment, next-generation manufacturing, and AI-enabled scientific advancement. It also addresses the need for streamlined permitting for AI infrastructure, grid modernization, semiconductor manufacturing revitalization, cybersecurity, and secure AI deployment in government and defense. Internationally, the plan calls for exporting American AI technology, countering adversarial influence in global governance, strengthening export controls, and aligning protection measures with allies to safeguard national security.

Accompanying the Action Plan, three executive orders were issued:

- Executive Order 14319 on Preventing Woke AI in the Federal Government: This order mandates that federal agencies procure only large language models that adhere to principles of truth-seeking and ideological neutrality.[42] It specifically prohibits the incorporation of diversity, equity, and inclusion ideologies that could distort factual accuracy or introduce partisan bias.
- Executive Order 14318 on Accelerating Federal Permitting of Data Center Infrastructure: This order directs federal agencies to expedite and streamline permitting and regulatory processes for large-scale AI data center projects and their supporting infrastructure.[43] The order also revokes Executive Order 14141, Advancing United States Leadership in Artificial Intelligence Infrastructure (Biden, January 17, 2025).
- Executive Order 14320 on Promoting the Export of the American AI Technology Stack: This order establishes a national program to promote the export of American AI technology packages, aiming to maintain U.S. leadership in AI and reduce reliance on adversary technologies.[44] It directs the Secretary of Commerce to create the American AI Exports Program, soliciting industry proposals for full-stack AI technology exports.



Collectively, these actions represent a significant federal shift toward a more unified, proactive, and security-focused approach to AI policy. While the Plan does not expressly preempt state laws, it directs the Federal Communications Commission to evaluate "whether state AI regulations interfere with the agency's ability to carry out its obligations and authorities[.]"[45]

### Limited Data Access Through Voluntary Standardization

Data access is critical to promoting and maintaining a vibrant AI ecosystem. Likewise, standardization efforts can encourage growth within the AI sector by facilitating exchange among industry actors and governmental entities. However, increasing concerns over data privacy have prompted legislation within the United States regulating the use of certain types of data. Striking the appropriate balance between promoting advancements in AI technologies and regulating potentially improper uses is likely to be a consistent challenge for U.S. policymakers for the foreseeable future.

At the forefront of the promotion and standardization efforts for AI data issues is NIST, created in 1901 and housed within the Department of Commerce. NIST's mission regarding AI is to research and develop standards for AI systems and data, with an emphasis on "cultivating trust in the design, development, use, and governance of artificial intelligence technologies and systems" (e.g., through research to ensure that AI technologies are explainable), as well as promoting AI innovation through technical standard-setting.

In response to the National AI Initiative Act of 2020, NIST also established and administers the National Artificial Intelligence Advisory Committee ("NAIAC"), which provides recommendations to the president on topics related to the current state of U.S. AI competitiveness, the state of the science around AI, and AI issues in the workforce, among others. One goal of the NAIAC is to develop broad access to high-quality data, models, and computational infrastructure necessary for AI research and development for the government and private sectors.

Part of developing this infrastructure involves developing a task force to implement a National AI Research Resource, which is envisioned as a shared computing and data infrastructure resource to provide AI researchers with access to computational services and high-quality data. The NAIAC, in this respect, has put out calls for voluntary data-sharing arrangements between industry, federal-funded research centers, and federal agencies; increased development in high-performance computing infrastructure; and cloud-based AI in an effort to advance AI research and technologies.

In addition to overseeing the NAIAC, on January 26, 2023, NIST published the Artificial Intelligence Risk Management Framework 1.0 ("AI RMF"), a guidance document to help manage AI's potential risks to individuals, organizations, and society. The AI RMF establishes the context for AI risk management, provides guidance on outcomes and activities to carry out the process of risk management to maximize the benefits while minimizing the risk of AI, and offers sample practices to be considered when developing and implementing AI products and systems. While voluntary for private industry, the AI RMF is consistent with global AI regulatory frameworks like the EU AI Act (discussed more below) and provides a roadmap that organizations can use to assess and comply with emerging oversight and risk management obligations.

In July 2024, NIST released AI 600-1,[46] "NIST AI Risk Management Framework for Generative Artificial Intelligence," which serves as a companion resource to the AI RMF. NIST AI 600-1 is specifically tailored to address the unique risks associated with GenAI and outlines the distinct risks posed by GenAI systems, such as confabulation, data privacy issues, and the potential for generating harmful or misleading content. It provides a comprehensive set of suggested actions for organizations to govern, map, measure, and manage these risks effectively across various stages of the GenAI life cycle. The importance of this release lies in its role in enhancing the trustworthiness, safety, and accountability of GenAI systems so that organizations can leverage the benefits of GenAI while mitigating potential harms. This aligns with the broader objectives of the NIST AI RMF to promote safe, secure, and trustworthy AI development and use. Notably, the White House's recent AI Action Plan calls for revising the NIST AI Risk Management Framework to "eliminate references to misinformation, Diversity, Equity, and Inclusion, and climate change," signaling a shift in federal priorities for AI governance.[47]

Legislative efforts to promote the development of AI have been proposed at both the federal and state level. In April 2021, the Senate introduced the Advancing American AI Act, which requires federal agencies to take steps to promote AI while ensuring that such developments align with U.S. values, including the protection of privacy, civil rights, and civil liberties. Specifically, the bill charges: the Office of Management and Budget with continually refining AI best practices and supporting modernization initiatives; the Office of Federal Procurement Policy with developing a process to ensure that AI contracts align with specific guidelines related to privacy; and the Department of Homeland Security with revising the process for procurement and use of AI-enabled systems to give full consideration to the civil rights impacted by such systems.

States have achieved varying levels of success in passing legislation directed to AI development. For instance, Alabama enacted State Bill 78, which established a Council on Advanced Technology and Artificial Intelligence to review and advise parties on the use and development of AI in the state, while a similar bill failed in Nevada. Some states are also encouraging investment in AI.

### Limited (State-Level) Regulation of Personal Data

While abundant data is critical to the successful development of AI-based technologies, the prospect of unregulated data collection of an individual's online interactions has long worried privacy advocates. In the United States, nationwide regulation for data protection exists only for specific data or segments of the population. For example, the Health Insurance Portability and Accountability Act ("HIPAA") governs how personal health information can be accessed and shared,[48] while the Family

Educational Rights and Privacy Act ("FERPA") accomplishes a similar function for students' private information. Outside of a handful of even more narrowly tailored legislation (e.g., the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Rule, etc.), most federal regulation of AI is concerned with potential discriminatory impact and appropriate market access for AI technologies, rather than the underlying data collection practices on which AI-based technologies rely.

In the absence of federal legislation, a growing number of states have passed laws to enable individuals to take more control over how their data is monitored and monetized online. California was the first to enact such legislation. The California Consumer Privacy Act ("CCPA") of 2018 mirrors the GDPR and provides consumers with the right to know what information is being collected and, subject to varying exceptions, the right to delete their personal information. Virginia was the second state to pass comprehensive data privacy regulations when it enacted the Consumer Data Protection Act in March 2021. Colorado soon followed with the Protect Personal Data Privacy Act in July 2021. The latter two acts mirror the CCPA and seek to give consumers more control over data collection. Other states have passed similar laws, and similar proposed bills on data privacy are currently pending in more states.[49]

In short, recent federal efforts in the United States have focused on promoting AI policy and standardization, leaving states to regulate data privacy. With regard to data accessibility for individuals, some consumers and privacy advocates have called[50] for more comprehensive legislation at the federal level. While the chances of a nationwide data privacy act seem increasingly likely, the political consensus to enact a specific piece of such legislation remains to be seen.

**Table 2–Summary of Main U.S. Data Access Regulations**

| Name of Legislation | Type of Data | Main Purpose | Effective Date |
|---|---|---|---|
| **General** | | | |
| **Privacy Act of 1974** | Personal data held by the U.S. government | Provides rules and regulations for the collection, use, and disclosure of personal information by U.S. government agencies | September 27, 1975 |
| **Federal Trade Commission Act** | N/A | Allows the FTC and other authorities to prosecute apps or websites that violate their privacy policies or engage in deceptive marketing language as it relates to privacy | September 26, 1914, and reorganized on May 24, 1950 |
| **Data-Specific** | | | |
| **Health Insurance Portability and Accountability Act** | Certain medical information | Protects protected health information held by covered entities | August 21, 1996 |
| **Fair Credit Reporting Act** | Credit report information | Restricts use of and access to information related to credit | October 26, 1970, and amended on December 4, 2003 |
| **Family Educational Rights and Privacy Act** | Student education records | Governs access to educational information and records by public entities | August 21, 1974 |
| **Gramm-Leach-Bliley Act** | Certain personal information | Governs the collection, use, and protection of consumer data held by financial institutions | November 12, 1999 |
| **Children's Online Privacy Protection Act** | Data from minors | Imposes certain limits on data collection for children under 13 years old | April 21, 2000, rule amended June 23, 2025 |

## CHINA

China has been actively working on systematic AI legislation. In 2024, the State Council published a legislative plan aiming to present a draft comprehensive AI law to the National People's Congress ("NPC"). Until then, AI regulation is managed through ad hoc regulations targeting specific issues. The Legislative Affairs Commission of the NPC is responsible for drafting the legislative plans, which includes soliciting views from various stakeholders to ensure comprehensive and effective legislation. On March 16, 2024, Chinese scholars unveiled a preliminary proposal that could shape forthcoming AI legislation drafts. In the interim, multiple government agencies and institutions have issued a series of relevant regulations and documents to promote the healthy development and regulated application of AI.

The PRC does not restrict AI's development or use in any AI-specific legislation. However, it is regulating elements essential for building AI technologies, including data (e.g., personal information, facial recognition, Big Data, algorithms, and automated decision-making).

### Data Protection

The PRC enhanced its regulation of data protection in 2021 by enacting the PRC Personal Information Protection Law ("PIPL").[51] Notably, consent is required to collect or otherwise process an individual's personal information unless one of a limited number of exceptions applies.[52] To use training data containing sensitive personal information (including facial and other biometric information), separate consent is required unless any of the exceptions apply and, per the National Standard GB/T 43697-2024 (which became effective on November 1, 2025), such consent must be obtained via a distinct affirmative action separate from acceptance of general terms. In addition, a personal information protection assessment, notice of the necessity and impact of processing, and strict confidentiality measures, such as encryption, are required. PIPL also forbids the use of automated decision-making to discriminate among individuals, for example by applying different contractual terms based on analyses of personal information such as habits, health, credit status, or financial situation.[53]

The PRC has enforced its Data Security Law and the Measures for Security Assessment of Outbound Data Transfer (2022),[54] under which certain data exports invite stricter regulations including security assessment for "important data" (with a broad and vague definition). The PRC Antitrust Law (amended in 2022) also stipulates that business operators may not use data, algorithms, or technology to engage in monopolization.[55]

In 2023, several governmental agencies, including the Cyberspace Administration of China ("CAC"), the National Development and Reform Commission, and the Ministry of Education, among others, issued and enforced the Interim Provisions on Management of Generative Artificial Intelligence Services ("Generative AI Provisions").[56] Accordingly, GenAI service providers are held accountable as "personal information processors" and are obliged to fulfill their obligations to protect personal information. GenAI service providers are restricted from unnecessarily collecting personal information or illegally disclosing users' prompts and usage records to third parties. AI users can request to access, copy, correct, supplement, or delete their personal information.

Additionally, AI service providers offering content-generating services are required to use data and foundational models from legitimate sources, protect personal information, respect intellectual property, enhance training-data quality, and report illegal content. On March 14, 2025, the CAC, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the National Radio and Television Administration unveiled the Measures for Labeling of AI-Generated Synthetic Content, effective on September 1, to prohibit AI-generated news content without explicit labeling as synthetic.[57]

The State Council promulgated the Network Data Security Management Regulations on September 30, 2024, which became effective on January 1, 2025. The Regulations cover the management and security of network data, which is crucial for AI systems that rely on large datasets for training and operation. Meanwhile, GenAI services are required to strengthen the security management of training data and training data processing activities and take effective measures to prevent and handle network data-security risks.

National standards and other technical documents promote voluntary standardization and provide guidance for the AI industry. For example, the Basic Security Requirements for Generative Artificial Intelligence Services,[58] published by the National Technical Committee 260 on Cybersecurity of

Standardization Administration of China, recommended security standards for training data and models used by GenAI providers, including not using information that is blocked by PRC laws or infringes intellectual property rights of others.

### Promotion of Data Flow

While data-security requirements are tightened, PRC regulators remain well-aware that promoting free flow of data is crucial to larger-scale application of AI. Promulgated by the CAC in March 2024, the Provisions on Regulating and Promoting Cross-Border Data Flow ("Data Flow Provisions")[59] are considered a significant adjustment from restrictions to a relief of compliance burdens. Specifically, the Data Flow Provisions aim to encourage data flow within protective legal frameworks by:

- Clarifying that if a data processor's data has not been noticed or publicly declared as "important data" by relevant governmental authorities, the data processor does not need to declare it as important data for security assessments;
- Providing exemptions for specific scenarios such as personal information entry and re-exit, international contracts involving individuals, cross-border HR management, and emergency assistance;
- Raising data amount thresholds that require AI developers to meet standard contract or certification requirements for personal information export; and
- Allowing new "free trade" zones for international data transfers. For example, Beijing[60] and Shanghai Lin-gang[61] free trade zones have each promulgated their own "negative lists" of data, exempting data outside these lists from certain regulatory requirements.

Significant data exports still face regulation. For example, entities in the Beijing free trade zone exporting audio or image data containing sensitive personal information of more than 50,000 individuals for model training, algorithm development, or product testing purposes must undergo security assessment. High-end chips, devices, or other technologies may also be considered highly confidential and restricted from sharing due to national security concerns.

## JAPAN

### Data Protection

In Japan, the use of personal information is regulated by the Act on Protection of Personal Information (Act No. 57 of 2003, as amended) ("APPI").[62] Under the APPI, consent is not required to collect personal information, except for sensitive personal information (such as health data). However, data subjects must either be notified of the purpose of the use of personal information, or the purpose of use must be published promptly after collection (unless it was already published in advance).[63] For transfer of personal data to a third party, the APPI requires data subjects' advance consent unless an exception applies.[64] Cross-border transfer of personal data also requires consent unless an exception applies.[65] The APPI's 2020 amendment has further heightened the consent requirement and now strictly requires more transparency in obtaining advance consent for international transfer of personal data. More specifically, a data-exporting entity must inform data subjects of: (i) the country where such third party is located; (ii) the personal information protection system of such country; and (iii) measures taken by such third party to protect the personal information.[66]

### Measures to Facilitate Data Collection and Flow

The strict consent requirement for the transfer of personal data can sometimes conflict with the business and innovation needs for collecting and analyzing vast amounts of data. The following legislation and governmental initiatives seek to address this issue.

- **Anonymously Processed Information.** By processing information in accordance with the strict processing rules set forth in the APPI implementation regulations and related guidelines, such that individuals cannot be identified, anonymously processed information[67] can be transferred to a third party without data subjects' consent, but the parties creating and using such information are subject to additional strict obligations and requirements.
- **Anonymized and Pseudonymized Medical Information.** Medical data is particularly useful for medical research and development, including the development of AI in relation to medical device and drug development (e.g., image diagnosis). However, the APPI imposes stricter regulations on the use of medical data than on other types of personal data. Collection of sensitive personal information, such as medical history, requires advance consent of the data subjects.[68] Further, the transfer restriction is also heightened, as the opting-out scheme that can apply to other types of personal data for transfer does not apply to medical data.[69]

  Additionally, Japan enacted the Act on Anonymized Medical Data and Pseudonymized Medical Data that Are Meant to Contribute to Research and Development in the Medical Field (Act No. 28 of May 12, 2017, as amended) ("Next-Generation Medical Infrastructure Act")[70] to facilitate use of anonymized personal medical data for medical research and development purposes. This act took effect with the relevant cabinet ordinances and guidelines on May 11, 2018. Under the act, medical institutions can collect and provide medical information to organizations certified to anonymize medical information without obtaining consent from patients, who oly need to be notified of certain required items only, including the patient's right to opt out.[71] The certified organization then anonymizes the medical information and can provide it to other organizations for use in medical research and development.

  On May 17, 2023, the Next-Generation Medical Infrastructure Act was amended to further relax the requirements for the use of personal medical information for research purposes. The amendment introduced a new framework for utilizing pseudonymized medical information, expanding its scope to include rare diseases and other unique data points. These changes took effect on April 1, 2024, along with the relevant cabinet ordinances and guidelines. Similar to the regulations governing anonymization of medical information, the amendment permits medical institutions to collect and provide medical information to organizations certified to pseudonymize medical information without obtaining explicit patient consent—patients need to be notified of certain required items only, including their right to opt out.[72] The certified organization then pseudonymizes the medical information and can provide it to other certified organizations for use in medical research and development.[73]

The strict consent requirement for transferring personal data under the APPI often deters AI developers from collecting more data, such as customers' marketing data and sales data, for the purpose of training AI models. To facilitate the development of AI with a balance of protecting personal data, the Japan Personal Information Protection Commission ("PPC") is currently discussing amendment of the APPI to permit the transfer of personal data, including sensitive personal information, to a third party without data subjects' advance consent if the data is used by the transferee for a general analytical purpose only, including creating statistics and developing AI. The relaxed requirements are intended to apply only when certain safeguards are in place, including publication of the name of the provider, the name of the recipient, and the purpose of the transfer (e.g., solely creation of statistics, training AI models) along with execution of an appropriate data-transfer agreement restricting the transferee's use of the personal data to such limited purpose. The PPC is also contemplating the introduction of administrative fines that may be imposed in the event of a large data breach or malicious use of personal data.

### Competition Regulation on Data Pooling and Lock-In

The Japan Fair Trade Commission prepared and published a "Report of the Working Group on Data and Competition Policy" on June 6, 2017.[74] The report confirmed that the current

Anti-Monopoly Act (Act No. 54 of April 14, 1947, as amended)[75] may apply to and regulate unfair data pooling and lock-in by monopolies and oligopoly firms (e.g., "unreasonable restraint of trade," "unfair trade practices").

## AUSTRALIA

### Minimal Regulation

While numerous bodies in Australia have stressed the need for AI regulation,[76] Australia does not yet have general laws and regulations specifically regulating the deployment and use of AI. However, many existing regulatory regimes can be applied to AI. In addition, a number of proposed reforms to introduce AI-specific laws and regulations are under active consideration.

### Proposed Mandatory Guardrails

The centerpiece AI-specific regulation that has been proposed in Australia is the proposed mandatory guardrails on AI use in high-risk settings. On September 5, 2024, the Australian federal government released the Proposals Paper for Introducing Mandatory Guardrails for AI in High-Risk Settings. The paper was developed with assistance from the temporary AI Expert Group, a multidisciplinary independent group that had been set up by the government to advise it on testing, transparency, and accountability measures for AI in legitimate but high-risk settings. This paper presented 10 proposed mandatory guardrails on the use of AI in "high-risk settings" for public consultation and sought submissions on the appropriate regulatory approach to such AI. These guardrails are general in operation and are relevant to data ecosystem, market access, and AI liability regulation.

The 10 mandatory guardrails are, in summary form:

1. Establish and publish an accountability process;
2. Establish a risk-management process;
3. Implement data governance measures to manage data quality and provenance;
4. Test and monitor AI model performance;
5. Ensure human control or intervention;
6. Inform end-users of AI-enabled decisions or content;
7. Establish mechanisms for users to challenge AI use or outcomes;
8. Be transparent with other organizations across the AI supply chain about data, models, and systems to help them effectively address risk;
9. Keep records to allow assessment of compliance; and
10. Undertake conformity assessments to demonstrate and certify compliance with guardrails.

"High-risk" settings are not clearly defined but are to be identified by reference to the following, broadly described principles:

- Risk of adverse impacts to an individual's rights recognized in Australian human-rights law without justification, in addition to Australia's international human-rights legal obligations;
- Risk of adverse impact to an individual's physical or mental health or safety;
- Risk of adverse legal effects, defamation, or similarly significant effects on an individual;
- Risk of adverse impacts to groups of individuals or collective rights of cultural groups;
- Risk of adverse impacts to the broader Australian economy, society, environment, and rule of law; and
- Severity and extent of those adverse impacts outlined in the above principles.

The guardrails will additionally apply to any general-purpose AI—defined as "an AI model that is capable of being used, or capable of being adapted for use, for a variety of purposes, both for direct use as well as for integration in other systems." The guardrails are proposed to apply both to developers and deployers of AI, encompassing individuals and organizations that supply or use an AI system in providing a product or service.

At least two of these guardrails are clearly directed toward the regulation of the data ecosystem: guardrail 3 and guardrail 8. Guardrail 3 ensures that the data that AI models are trained on is legally obtained, high quality, reliable, and fit-for-purpose. This regulation is also aimed to protect the security of data used. It provides a direct nexus between existing information and intellectual property legislation, such as the Privacy Act 1988 (Cth), the Security of Critical Infrastructure Act 2018 (Cth), and the Copyright Act 1968 (Cth), and the use of data in AI

systems. It is described by the Australian federal government as consistent with the EU AI Act's requirement that general-purpose AI comply with copyright law and the ISO/ISE 42001, so implementation of this proposal would likely entail similar standards.

Guardrail 8 is designed to allow AI supply chains to cooperate in identifying and mitigating AI use risks, as well as ensuring legal obligations are being met. It would require deployers to report adverse incidents and, as with Guardrail 3, is intended to align with the EU AI Act's requirement of transparency and provision of information to AI deployers.

The consultation process for the proposed guardrails closed on October 4, 2024, but it remains to be seen whether these proposals will find their way into law or, if they do, what form these mandatory regulations will ultimately take.

### Voluntary AI Safety Standard

Simultaneous with the proposal for the mandatory guardrails, the Australian federal government released 10 voluntary guardrails, which businesses can seek to comply with now in anticipation of further regulation. This voluntary standard is intended to reflect international best practices and is to be updated over time to conform with changes in international best practice. Organizations that have implemented the voluntary guardrails will be well-positioned to comply with mandatory guardrails legislation, if and when it is passed into law.

The Voluntary AI Safety Standards are identical to the mandatory guardrails, with the exception of standard 10, which reads (unlike guardrail 10): "Engage your stakeholders and evaluate their needs and circumstances, with a focus on safety, diversity, inclusion and fairness." No legal penalties are associated with a failure to meet these standards.

### Existing Legislative Schemes

Many existing legislative regimes have potential application to AI use and development in Australia, notably including:

- The Privacy Act 1988 (Cth), which contains restrictions on the use and storage of personal information (for organizations with an annual turnover of more than AU$3 million). The application of the Privacy Act to AI is more than hypothetical. On November 2, 2021, the Office of the Australian Information Commissioner determined that Clearview AI had breached Australian privacy law by scraping biometric information from the web and disclosing it through a facial recognition tool. Clearview AI was ordered to cease collecting facial images from Australians and destroy existing images collected from Australia.
- The Copyright Act 1968 (Cth). In the absence of any general fair-use defense as it exists under U.S. law, both the training of AI models and their output may infringe third-party materials protected by copyright. In addition, Australian copyright law requires a human author in order to prove copyright subsistence. As such, works created wholly by GenAI will not be protected under Australian law. Whether the law should be changed in some way to protect such works, and the extent to which Australian copyright law will protect works that involve human authorship in combination with the use of GenAI, are matters currently under discussion.
- The Patents Act 1990 (Cth). Similar issues arise under Australian patent law. For example, in 2022 the High Court held that an invention is patentable under Australian law only if the inventor is a natural person.[77] The Australian Patents Office is currently considering the implications of AI for Australian patent law, particularly in relation to inventorship issues (including situations where one or more human inventors materially contribute to an invention created with the assistance of AI).
- The Australian Consumer Law (ACL), which prohibits (among other things) misleading or deceptive conduct, unconscionable conduct, and false or misleading representations.

These laws have a very wide scope of application. For example, the Australian Department of Industry, Science, and Resources has warned about their applicability in connection with unfair data collection and use practices. The application of these laws to computational algorithms has already featured in at least one action brought by the regulator (the Australian Competition and Consumer Commission) against Trivago (*see* further below).[78]

### Novel Legislative Reforms

Existing legislative regimes are also being amended to shape their application to AI data ecosystems.

On September 19, 2024, the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 (Cth) was introduced to Federal Parliament, proposing to amend the Broadcasting Services Act 1992 (Cth) to impose obligations on digital communications platform providers in relation to the dissemination of content on digital communications platforms that is verifiably false, misleading or deceptive, or reasonably likely to cause or contribute to serious harm. While not directly targeted at AI content, the bill would in effect place obligations on digital communications platform providers to moderate and control AI content on their platforms to avoid violating these proposed laws.

As a result of legislative and community opposition to the proposed reforms, in early December 2024, the Australian federal government announced that it had decided not to proceed with this reform proposal at the present time. The bill later lapsed when a federal election was called in March 2025. While the Australian government was returned with an increased majority at the election held in May 2025, it remains to be seen whether these or similar reform proposals will be reintroduced in the new parliament and, if so, whether those reforms are likely to find majority support in the upper house.

On February 16, 2023, the Federal Attorney-General's Department released the report from its review of the Privacy Act. The report included recommendations responding to the data risks posed by the modern digital economy, in particular the collection and storage of huge amounts of personal data. On September 12, 2024, the Privacy and Other Legislation Amendment Bill 2024 (Cth) ("Privacy Act Amendment Bill") was introduced to Federal Parliament, implementing the first tranche of agreed recommendations from this review. Among the reforms relevant to the AI data ecosystem is the establishment of a children's online privacy code applying to social media and other internet services accessed by children. It imposes distinct privacy obligations in relation to children and expands the regulatory powers of the Information Commissioner to investigate and seek enforcement against a breach of privacy law.

The Privacy Act Amendment Bill passed both houses of Australian Parliament in late November 2024 and received royal assent on December 10, 2024. Now known as the Privacy and Other Legislation Act 2024 (Cth), the Act will require organizations to update their privacy policies to disclose when decisions are made using automated processes (effective December 10, 2026) and will require the Office of the Australian Information Commissioner to develop a code addressing online privacy for children.[79] It will introduce enhanced obligations for online services that are directed to, or likely to be accessed by, children.

## MARKET ACCESS

Regulators' concerns that certain AI systems could in some instances pose risks to safety or fundamental rights have spurred countries to regulate how such systems can access the market. The asserted risks at stake typically depend on the goal pursued and the area where the AI is used. For example:

- Algorithms that have the purpose or effect of enabling price cartels may be caught by antitrust laws.
- Certain large-scale uses of facial recognition technology may trigger questions related to privacy, consent, and individual rights, as shown by the restrictions imposed on Clearview's technology.[80]
- The use of AI systems in selecting job applicants or determining the creditworthiness of borrowers may raise issues related to statutory antidiscrimination protections. Allegations may focus on various factors. For instance, an algorithm may be trained with a historic dataset that is identified as reflecting bias, amplifying past discriminatory hiring practices. Similar effects might also arise from the underrepresentation of a group in the dataset or the selection of analyzed characteristics.

Rules on market access for AI systems could be focused on limiting such risks and the subsequent harm caused. This might include adapting existing legal frameworks to the specificities of AI systems, but also creating tailored AI market-access legislation.

## EUROPEAN UNION

### Current and Former Legislation

An extensive body of existing EU product safety legislation potentially applies to various AI applications, but attempting to apply this existing legislative framework to new AI systems has raised various problems. For instance, the General Product Safety Directive (dating from 2001) had a limited scope that applied only to products, thereby potentially excluding AI-based services such as those related to health, financial, or transport services.

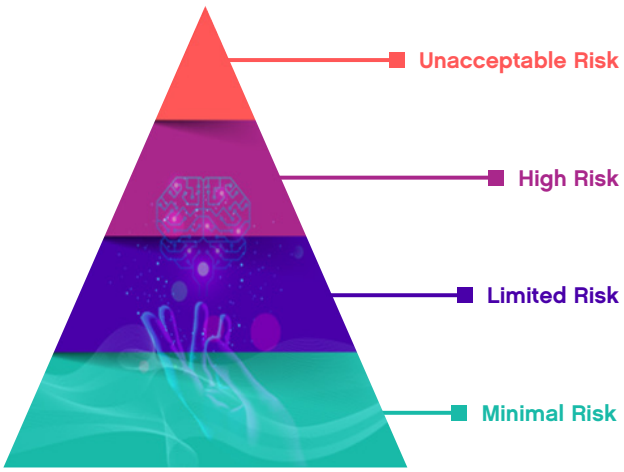
In setting out an AI strategy,[81] the European Union sought to promote the uptake of AI while addressing the associated risks. One important aspect is regulating market access while ensuring user safety and safeguarding fundamental EU values and rights. After recognizing loopholes in the existing product safety legislation, the European Commission took action in April 2021 to ensure the safety of AI placed on the market. In addition to its Coordinated Plan on AI[82] outlining necessary policy changes and investment at the Member State level, the Commission also set out regulations aimed at harmonizing safety requirements and market access of AI applications at the EU level, including: (i) the AI Act;[83] (ii) the General Product Safety Regulation[84] (to replace the General Product Safety Directive); and (iii) the Cyber Resilience Act.[85]

### EU AI Act

On August 1, 2024, the EU AI Act entered into force, with the goal of fostering responsible AI development and deployment in the European Union. Proposed by the Commission in April 2021 and subsequently ratified by the European Parliament and the Council in December 2023, the EU AI Act aims to mitigate potential risks to health, safety, and fundamental rights by delineating explicit requirements and obligations for developers and deployers concerning specific AI applications, while simultaneously alleviating administrative and financial burdens for businesses.[86]

Under the EU AI Act's risk-based approach (see figure below):

- Certain AI practices are prohibited, as they are considered a central threat to fundamental rights (e.g., this includes social scoring by governments but not "killer robots").
- Certain AI systems are classified as high-risk and subject to conformity assessment procedures before they can be placed (or put into service) on the EU market. High-risk AI includes: (i) AI used for products already covered by specific EU product safety legislation, such as for machinery, toys, radio equipment, cars and other types of vehicles, and medical devices; and (ii) AI used in certain contexts, such as safety in the management and operation of critical infrastructures, human resources, and creditworthiness assessments. High-risk AI is also subject to specific obligations such as data governance, human oversight, and transparency.
- Certain low-risk AI systems, like deepfakes or chatbots, are subject to harmonized transparency rules.




| | |
|---|---|
| **Prohibited** | e.g., social sorting by government |
| Permitted subject to **conformity assessment** and obligations | e.g., recruitment, credit scoring, safety components in critical infrastructure |
| Permitted subject only to **transparency** obligations | e.g., deepfake, chatbots |
| Permitted with no obligations | e.g., spam filter, AI-enabled video games |

Eur. Comm'n, Shaping Europe's Digital Future.

With regard to enforcement, national regulators may conduct market monitoring and surveillance and are empowered to impose significant fines. These activities are overseen by the European AI Office, which was established in February 2024 within the European Commission in Brussels.

Although the EU AI Act came into force on August 1, 2024, obligations apply in phases: prohibitions and AI literacy from February 2, 2025;[87] GPAI model obligations and governance rules from August 2, 2025; most remaining requirements from August 2, 2026; and high-risk AI rules for systems embedded in regulated products subject to existing EU product safety legislation (e.g., medical devices) from August 2, 2027.

### Preventing Biases

The EU AI Act[88] aims at resolving, in particular, the issue of biases allegedly created or amplified by AI. Bias and discrimination are inherent risks of any societal or economic activity, including for AI systems. However, AI's large scale means that the impact of its shortcomings could be much greater and more systematic, thus increasing the impact risks. Allegations of AI-based biases typically result from either the use of low-quality training data or AI system opaqueness that can make it difficult to identify possible flaws in the AI system's model or algorithmic design.

While the GDPR rules already address bias issues (e.g., through its data accuracy obligation under Article 5(1)(d) and prohibition of decision-making based solely on profiling under Article 22), the EU AI Act further limits bias risks. Its high-risk AI requirements minimize the risk of algorithmic discrimination, particularly in relation to the quality of datasets used for developing AI systems and its obligations for testing, risk management, documentation, and human oversight throughout the entire AI system's life cycle (Articles 9–15). In addition, the EU AI Act imposes transparency requirements on providers of general-purpose AI models, requiring disclosure of a summary of the training data used in the model's development.[89]

### General Product Safety Regulation

To keep pace with technological developments, the European Union has adopted the General Product Safety Regulation,[90] which replaced the General Product Safety Directive in December 2024. The new General Product Safety Regulation represents a shift in the status of substantive law from a directive to a regulation. Consequently, it will directly affect Member States, obviating the need for national transposition legislation. The Regulation aims to broaden the current Directive's scope to cover, in particular, AI systems. As mentioned above, the General Product Safety Directive's limited scope applied only to products and did not cover AI-based services. The Regulation expands certain definitions, such as "product," to enable regulating new technologies. It encompasses both general consumer products and, more specifically, AI-enabled consumer products. However, there is reason to conclude that stand-alone AI software falls outside the scope of the General Product Safety Regulation, although the law may capture embedded software and safety risks from updates. This issue was previously contentious under the General Product Safety Directive.

### Cyber Resilience Act

The Cyber Resilience Act[91] is a legal framework that provides cybersecurity requirements for hardware and software products with digital elements placed on the EU market. The Council adopted the Cyber Resilience Act on October 10, 2024. As a horizontal piece of EU legislation, the Cyber Resilience Act will generally apply only where more specific EU legislation (the *lex specialis*, such as the AI Act) does not impose more detailed cybersecurity requirements. However, with respect to high-risk AI systems, the Cyber Resilience Act explicitly provides that products with digital elements (also considered high-risk AI systems under the EU AI Act) will be deemed to comply with the cybersecurity requirements of the EU AI Act if they meet the essential cybersecurity requirements set out in the Cyber Resilience Act ("secure-by-design"). The Cyber Resilience Act entered into force on December 10, 2024, and the main obligations of the act become applicable on December 11, 2027. The provisions for vulnerability and incident reporting become applicable on September 11, 2026. For products with digital elements that are also high-risk AI systems, fulfilling the Cyber Resilience Act's essential cybersecurity requirements is deemed to satisfy the EU AI Act's cybersecurity requirements (without prejudice to accuracy/robustness), provided this is demonstrated in the EU declaration of conformity. The presumption of conformity applies only to the cybersecurity aspects. A high-risk AI system must still meet the other EU AI Act's requirements related to accuracy, robustness, and overall fundamental safety that are not covered by the Cyber Resilience Act.

### Other Relevant Legislation

Various other sector-specific legislative instruments, which do not focus solely on AI, could also be relevant for market access of AI-related products, including to the extent that these rules facilitate cross-border trade. These include the EU Cybersecurity Act,[92] in force since 2019, which establishes an EU-wide cybersecurity certification framework for information and communication technology products, services, and processes; the Regulation on Medical Devices,[93] in force since 2017, whose rules govern software medical devices; and the Regulation on In-Vitro Diagnostic Medical Devices,[94] in force since 2017.

## UNITED KINGDOM

### AI Legal Framework

In contrast to the European Union, the United Kingdom has not yet proposed a single overarching AI regulation. Instead, it currently relies on existing laws and sector-specific regulations, supplemented by guidelines and ethical frameworks. In August 2023, the outgoing Conservative-led government issued a policy paper on the United Kingdom's approach to the regulation of AI.[95] This paper outlined a framework based on five principles (safety, security, and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress). These principles were not intended to be put on a statutory footing initially. Instead, the government intended that regulators would, at a future point, be put under a statutory duty to have regard for these principles. However, following the change of government in 2024, it is anticipated that the United Kingdom will depart from the nonprescriptive approach to AI regulation and will instead adopt a binding set of AI measures.

In December 2024, the UK government initiated a consultation on Copyright and Artificial Intelligence.[96] The consultation aims to address the interplay between copyright law and AI. Currently, the application of UK copyright law to the training of AI models remains ambiguous, presenting potential challenges for both AI developers and rights holders. The consultation proposes transformative updates to the United Kingdom's statutory framework, including:

- Updates to the text and data-mining section (addressed further below);
- Enhancements to transparency requirements for AI training;
- Assessment of the use of collective licensing regimes to assist rights holders with remuneration;
- Consideration of whether AI outputs should be labeled;
- Evaluation of whether the current statutory protection for purely computer-generated works should be reformed; and
- Addressing concerns regarding the emergence of digital replicas (i.e., deepfakes).

The consultation closed on February 25, 2025, and is expected to result in an updated copyright framework that aligns more closely with recent developments in the European Union.

In January 2025, the UK government announced the AI Opportunities Action Plan,[97] which outlines a three-stage strategy: (i) laying the foundations to enable AI; (ii) transforming lives by embracing AI; and (iii) securing the United Kingdom's future with "homegrown" AI. This plan supports the government's "pro-innovation" approach to AI adoption, aiming to boost economic growth.

In March 2025, the Artificial Intelligence (Regulation) Bill [HL] (2025) ("AI Bill")[98] was reintroduced by Lord Holmes. The AI Bill had previously failed to be tabled during the last parliamentary session due to the dissolution of Parliament following the 2024 UK election. This private member's bill proposes the establishment of an "AI Authority" tasked with ensuring regulatory accountability in delivering the five principle-oriented approach. Although private member's bills are rarely enacted, the AI Bill offers a legislative framework designed to assist the government in implementing a cohesive and safety-oriented regulatory approach to artificial intelligence in the United Kingdom; it may therefore act as a helpful guide for future AI legislation.

### Regulatory Oversight

To date, the United Kingdom's key market regulators have issued a wide range of guidelines and policy papers on the approach to AI regulation. A cohesive regulatory approach can be observed through the introduction of the Digital Regulation Cooperation Forum ("DRCF") in 2020.[99] The DCRF brings

together four UK regulators: the Competition and Markets Authority ("CMA"), the Financial Conduct Authority ("FCA"), the ICO, and the Office of Communications ("Ofcom"). This forum was created to enhance cooperation and coordination among these regulators, ensuring a coherent and responsive regulatory approach to AI in the UK digital economy.

The primary aim of the DRCF is to facilitate effective collaboration among its member regulators on digital regulatory AI matters. For example, the DRCF undertakes a range of research, policy development, and stakeholder engagement activities. In April 2024, the DRCF launched a 12-month pilot called the DRCF AI and Digital Hub,[100] which enables businesses to submit cross-regulatory queries on AI-related products. The purpose of the Hub was to provide informal advice to businesses developing AI systems, which is turned into anonymized guidance for other businesses. This will undoubtedly be a pivotal resource for advising on UK AI regulation in the future.

### Financial Markets Regulation

The FCA released its "AI Update" in 2024,[101] reflecting upon the previous government's principles-based approach to regulation. It is unclear whether the FCA will update its position following the Labour government's anticipated 2025 AI legislation. Nonetheless, the FCA's update noted the importance of: (i) understanding AI development and how it is deployed within UK financial markets; (ii) monitoring and adapting the regulatory framework to identify material changes impacting consumers and markets; and (iii) collaborating with other regulators through the DRCF to build consensus on best practices and potential future regulatory work. The FCA's AI Update mapped the FCA's existing regulatory frameworks to the five principles discussed above. In particular, the FCA's Consumer Duty would already address some of the potential harms that could be caused to consumers depending on how firms used AI. This has been somewhat helpful for compliance professionals to understand how the FCA has viewed the overlap between its existing rules and the five AI principles. However, the lack of granularity from the FCA (and other UK regulators) about precisely what financial services firms need to do in order to meet regulatory expectations leaves significant residual risk for firms trying to incorporate (or who have already incorporated) AI into their products and operations. In October 2024, the FCA's Innovation Hub announced an AI Lab to provide "a pathway for the FCA, firms and wider stakeholders to engage in AI-related insights, discussions and case studies."[102]

### CMA

The CMA's most recent guidance from April 2024[103] provides an initial assessment of the competitive risks of AI and how it intends to develop a response system to these risks. The update spotlights the risks of AI rapid price-fixing and consumer profiling to give certain products "undue prominence" in online retail spaces. Significantly, however, the CMA has not yet committed to any concrete plans.

### UK AI Assurance Market

In November 2024, the UK government announced[104] a significant expansion in the AI assurance market, projecting a six-fold growth by 2035, which is expected to unlock more than £18.8 billion.[105] This growth is part of the UK government's broader strategy to integrate AI into public services and the economy while ensuring public trust through robust assurance mechanisms. The AI assurance market currently comprises around 524 firms employing more than 12,000 people and generating more than £1 billion. To support this growth, the UK government is launching a new AI Assurance Platform that will serve as a comprehensive resource for businesses to identify and mitigate AI-related risks. This platform will provide guidance on conducting impact assessments, evaluating data for bias, and implementing responsible AI management practices, particularly benefiting small and medium-sized enterprises. The UK government has also promoted AI assurance growth and expanded international safety collaboration (e.g., the AI Safety Institute agreement with Singapore, Nov. 2024).

### Trial Government AI Scheme

In November 2024, the Department for Science, Innovation, and Technology released an update regarding the trial of a government-generated chatbot, GOV.UK Chat.[106] The chatbot, designed to assist small businesses with navigating complex government advice, will be tested by up to 15,000 business users. This follows earlier trials where nearly 70% of users found the tool helpful. The chatbot, built using OpenAI's GPT-4o technology, aims to provide personalized and straightforward answers by collating information from various GOV.UK pages. The trial will link the chatbot to 30 business-related

pages, allowing users to ask questions about tax and business support.

This trial is part of a broader initiative by the Science Secretary to integrate emerging technologies into government services, aiming to reduce bureaucratic inefficiencies. Stringent safety measures, including "guardrails" to prevent inappropriate responses, have been implemented. User experience improvements, such as onboarding processes and enhanced accessibility, have also been made. The trial's outcomes will guide further developments to ensure the chatbot meets high accuracy standards and effectively supports public service innovation.

### AI Safety Institute

The AISI recently signed a new agreement with Singapore[107] to enhance research and develop shared standards for AI safety. This partnership builds on commitments made at the AI Safety Summit and aims to align efforts on research, standards, and testing through the International Network of AI Safety Institutes. The AISI has also launched the Systemic AI Safety Grants program, offering up to £200,000 in funding for researchers. These efforts underscore the United Kingdom's commitment to becoming a global leader in AI safety and assurance, ensuring that AI technologies are developed and deployed responsibly.

### Text and Data Mining

A pivotal area on the authorization of data used to train AI models is the law on text and data mining ("TDM"). Since TDM relies on copying large amounts of digital material, it is subject to copyright law in the United Kingdom and currently requires either permission from rights holders or to fall within an exception permitted by statute. Specifically, AI developers will look toward the TDM exception outlined in section 29A of the Copyright, Designs and Patents Act 1988 ("CDPA 1988"),[108] which was introduced in 2014. This exception permits TDM on the following conditions:

- The person conducting TDM must have lawful access to the work (e.g., through a subscription or purchase), and the use must not be restricted by contractual terms imposed by the rights holder;
- The use must be for the purpose of noncommercial research; and
- The work must be accompanied by sufficient acknowledgment unless this is impossible for reasons of practicality.

Section 29A continues by expressly stating that where a copy of a work has been made via an authorized TDM, that work will be infringed if it is: (i) "transferred to any other person," except where the transfer is authorized by a copyright owner; or (ii) if the copy is used "for any other purpose." The TDM exception should therefore be construed narrowly and for noncommercial purposes. Accordingly, if a commercial AI developer copies or uses data collected by an authorized entity (e.g. a research organization), copyright infringement will be deemed to have occurred if the original copyright owner's consent was not obtained when making that copy.

The UK government's consultation on Copyright and AI has reintroduced a proposal to broaden the TDM exception. Initially proposed in 2021, this idea faced significant resistance from the creative industries. In the most recent consultation, the UK government has suggested an opt-out model similar to the TDM mechanism in the European Union. This opt-out proposal would allow AI developers to use copyrighted works for training purposes unless rights holders have issued a reservation to prevent their work from being used. The practicalities of an opt-out mechanism require further detail, which the consultation does not currently address. Additionally, by introducing more developer-friendly training mechanisms, the United Kingdom aims to restore some balance for rights holders by suggesting that greater transparency guidelines be required for AI developers. These guidelines would necessitate developers to reference works used to train their models, thereby ensuring compliance with the opt-out regime.

Presently, the most assured way for an AI developer to conduct TDM in the United Kingdom would be through licensing arrangements with copyright owners.

## UNITED STATES

### Patchwork of Competent Authorities

Federal enforcement authorities have expressed concerns over the potential misuse of AI-based technologies, especially as such misuse might affect individuals. Congress has yet to enact any new legislation concerning AI, and, accordingly, the scope and validity of federal action to regulate AI remains

uncertain. This stands in contrast to the comprehensive efforts to categorize and prohibit certain forms of AI as proposed in the European Union.

At the federal level, the FTC was one of the first agencies to assert a role in preventing the misuse of AI-based technologies under Section 5 of the FTC Act and existing laws for AI-related deception, unfairness, and discrimination, and it recently reaffirmed its intentions to be active in regulating AI when it launched Operation AI Comply in September 2024.[109] The FTC claims to draw its asserted authority to curb discriminatory AI-based practices from section 5 of the FTC Act, which prohibits unfair or deceptive practices; the Fair Credit Reporting Act; and the Equal Credit Opportunity Act. The FTC had previously noted in a blog post that it can file a complaint for even inadvertent violations, such as when a company's AI algorithm results in credit discrimination against a protected class.

While these theories remain controversial, the FTC has moved ahead with enforcement actions over the past year. In a recent complaint, the FTC asserted that Rite Aid, through its implementation of facial recognition technology aimed at loss prevention in its retail stores, failed to implement adequate safeguards to prevent discriminatory misidentification of individuals with prior shoplifting behavior.[110] With the new administration, it remains to be seen if the FTC will follow through on its warning for companies to "hold yourself accountable—or be ready for the FTC to do it for you."[111]

Other federal agencies have also voiced their perceived roles in regulating market access and certain forms of AI prohibition, typically in relation to the potential for discrimination against a protected class. For example:

- The CFPB controversially asserted in March 2022 that its "unfairness" authority may also be used to regulate discriminatory use of AI, such as in credit denials or home appraisals. According to CFPB Director Rohit Chopra (formerly an FTC Commissioner), "Companies are not absolved of their legal responsibilities when they let a black-box model make lending decisions." This interpretation, however, was held to exceed the agency's statutory authority by a Texas federal court in 2023. The CFPB appealed the district court's decision to the Fifth Circuit, but in April 2025, the parties jointly agreed to stipulate to the dismissal of the CFPB's appeal.[112]

- The Equal Employment and Opportunity Commission announced the launch of the Initiative on AI and Algorithmic Fairness in October 2021. The Initiative is set to examine the use of AI in the hiring and employment process against existing civil rights laws—many of which were enacted decades before the advent of AI.
- Similarly, the Department of Housing and Urban Development ("HUD") released guidance on the use of AI in housing decisions in May 2024. Per HUD, "[h]ousing providers, tenant screening companies, advertisers, and online platforms should be aware that the Fair Housing Act applies to tenant screening and the advertising of housing, including when artificial intelligence and algorithms are used to perform these functions."
- The FHFA released an advisory bulletin in February 2022 that provides AI and machine-learning risk-management guidance for Fannie Mae and Freddie Mac. It is the first publicly released guidance by a U.S. financial regulator that is focused on AI risk management.
- In 2025, the DOJ finalized its Data Security Program ("DSP") implementing Executive Order 14117 to restrict bulk sensitive data transfers to countries of "concern" (such as China, Russia, North Korea, Venezuela, etc.),[113] which will limit access to certain U.S. bulk data for training. This program became effective on April 8, 2025. The DSP restricts or prohibits certain transactions involving bulk U.S. sensitive personal data or government-related data with designated "countries of concern" or "covered persons" affiliated with those nations.

- Finally, the U.S. Department of the Treasury also issued a final rule on its Outbound Investment Security Program (Outbound Investment Rules) in October 2024 to implement Executive Order 14105. This rule became effective on January 2, 2025 and prohibits or requires notification of certain U.S. investments in Chinese-affiliated companies involved in specific national security technologies and products, including semiconductors and microelectronics, quantum information technologies, and artificial intelligence.[114]

### Legislative Activity

The U.S. legislative approach to AI prohibition is likewise piecemeal and predominantly issue-driven. At the federal level, lawmakers have proposed legislation focused on: (i) restricting the use of GenAI to produce political ads with false or misleading content;[115] (ii) protecting individuals' name, image, and likeness rights;[116] (iii) limiting the use of AI to monitor employee activity;[117] and (iv) calling for greater transparency, accountability, and security in AI applications while promoting innovation.[118] Lawmakers have also drafted legislation seeking to provide governance of AI use by federal agencies.[119] To date, no comprehensive federal AI regulation has been enacted.

At the state level, however, lawmakers have made more progress in regulating the use of AI by both public and private entities. More than a dozen states have enacted bills authorizing studies or committees seeking to better understand the impact of AI and the need for regulation, such as Colorado's Artificial Intelligence Impact Task Force. Several states, including California and Maryland, have also imposed additional requirements on state agencies seeking to leverage AI in their operations.[120]

Extending to the private sector, lawmakers across the United States have enacted or are considering laws that require companies to conduct impact assessments or otherwise provide justification that a proposed use of AI is safe and does not violate civil rights. Colorado, California, and Illinois are leading the way in this effort, having already enacted Colorado Senate Bill 24-05 ("Colorado AI Act"), California Senate Bill 942 ("California AI Transparency Act"), and Illinois House Bill 3773, respectively.

The Colorado AI Act, enacted in May 2024 and effective in June 2026, is the first comprehensive state law to provide a framework for the safe, transparent, and fair development and deployment of high-risk AI systems.[121] The law imposes disclosure, governance, and risk analysis obligations for companies. It defines "high-risk" AI systems as any system that, when deployed, makes or is a substantial factor in making a "consequential decision." Such consequential decisions may relate to employment, healthcare, or financial services. Meanwhile, Illinois House Bill 3773, enacted in August 2024 and effective January 2026, prohibits employers from using AI in a way that results in discrimination against others based on protected characteristics, such as race, ethnicity, or gender. It also requires companies to provide notice when AI is being used for employment decisions, such as hiring or promotion.[122]

Narrower legislation focused on specific industries or uses, such as landlords (concerned with rental price fixing or housing discrimination) and insurance providers (both health care and casualty insurance), have also been proposed. A particular focus for state lawmakers has been requiring transparency in the use of AI, from regulating the use of GenAI in political ads,[123] requiring notice of AI use in health care provision or insurance decisions, and requiring notice of AI use in hiring or employment decisions.

For example, the California AI Transparency Act, effective January 2026, requires that companies develop and adopt output generation and detection tools to facilitate watermarking and transparency for users.[124] Likewise, California's Generative Artificial Intelligence Training Data Transparency Act, effective January 2026, requires developers of GenAI systems to publicly disclose detailed information about the data used to develop their AI models.[125] Looking more broadly, proposed legislation seeks to prohibit AI that violates civil rights or existing legal protections, as well as ensuring individuals have knowledge if they may have been adversely affected by AI discrimination or bias.

### Executive Action

In addition to legislative action, the White House has issued multiple directives to shape AI policy and market access. For example, on January 23, 2025, President Trump signed Executive Order 14179,[126] titled "Removing Barriers to American Leadership in Artificial Intelligence," calling for development of an action plan to "promote human flourishing, economic competitiveness, and national security" within six months. Executive Order 14179 seeks to reduce bureaucratic barriers, enabling faster deployment of AI technologies across various sectors. Notably, it also directed federal agencies to review

and rescind all actions taken pursuant to Executive Order 14110, which President Biden signed on October 30, 2023, that are found to be inconsistent with the action plan's policy objectives.

Pursuant to Executive Order 14179, the Office of Management and Budget released a memorandum on "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust"[127] on April 3, 2025. The memorandum directed all federal agencies to adopt a "forward-leaning and pro-innovation approach" to AI in shaping the future of government operations, including directives to: (i) develop and publish strategies for implementing AI; (ii) improve AI governance and establish policies for "consequential decision-making"; and (iii) implement risk-management practices governing AI use that protect the public trust. The Department of Homeland Security also released the "Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure" in November 2024, providing guidance on the safe and secure development of AI in critical infrastructure.[128]

The Trump administration's Executive Order 14179 reflects some, but not complete, change in policy approach to AI regulation and adoption, which includes the aim of removing "ideological bias" in AI systems. President Biden's Executive Order 14110 marked the first attempt by the federal government to develop a comprehensive framework by which to manage the risks resulting from the rapid development of AI, and it directed NIST to develop standards for the safe and secure development and evaluation of AI systems. Its subsequent rescission underscores President Trump's shift away from the previous administration's focus on AI safety and oversight in favor of fostering rapid AI technological progress.

Executive Order 14110 ("Advancing U.S. Leadership in AI Infrastructure"), issued on January 14, 2025,[129] was ultimately rescinded on July 23, 2025, with President Trump's Executive Order 14318 ("Accelerating Federal Permitting of Data Center Infrastructure").[130] Yet some of President Biden's initiatives remain in effect. For example, OMB Memorandum M-25-03 ("Federal Data Center Enhancement"), issued alongside Executive Order 14141, provides guidance to federal agencies on optimizing data center operations, focusing on energy and water efficiency. Executive Order 14144 ("Strengthening and Promoting Innovation in the Nation's Cybersecurity") emphasizes the integration of AI in enhancing cybersecurity measures and remains in effect under the Trump administration.

The Biden administration's White House Office of Science and Technology Policy published on October 4, 2022, the "Blueprint for an AI Bill of Rights" (the "AI Bill of Rights"), which also remains in effect. The AI Bill of Rights is a set of voluntary and nonbinding guidelines with the stated purpose of protecting the public from harmful outcomes or harmful use of technologies that implement AI.[131] The AI Bill of Rights' framework applies to companies with "(1) automated systems that (2) have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services." Companies falling under this framework are encouraged to follow the five principles outlined in the AI Bill of Rights:

- **Safe and effective systems.** Companies should ensure automated systems are designed to protect users from harm and that such systems are monitored to identify and mitigate safety risks.
- **Algorithmic discrimination protections.** Companies should emphasize equity when developing algorithms through use of representative data and by conducting proactive equity assessments.
- **Data privacy.** Users sharing their data should have agency over how their data is used and be protected from abusive data practices, and companies should limit collection to data that is "strictly necessary for the specific context."
- **Notice and explanation.** Users should be notified when an automated system is in use, and accessible plain language should describe how and why such a system contributes to outcomes that impact users.
- **Human alternatives, consideration, and fallback.** Companies should provide users with the option to opt out from automated systems and alternatively provide access to a human consultant, where appropriate.
- **Children's privacy.** The FTC's COPPA Final Rule[132] amendments were published on April 22, 2025, and took effect June 23, 2025. Under these amendments, operators have until April 22, 2026, to comply (with some earlier dates for certain safe harbor obligations). The amendments update notice content, retention, and data-security program requirements, and clarify limitations on behavioral advertising to children.

While the AI Bill of Rights itself was not directly targeted at companies, it provided a values-based framework for evaluating AI risks and impacts that some agencies and firms have used as a reference. In 2025, U.S. federal policy emphasis has shifted toward the AI Action Plan and agency-specific tools (e.g., NIST's AI RMF profiles, DOJ data-security rules). The rescission of Biden's Executive Orders 14110 and 14141, which emphasized AI safety and ethical considerations, signals a move toward a more innovation-centric approach, potentially deprioritizing the principles outlined in the AI Bill of Rights.

## CHINA

### Promoting AI

The PRC states in its Law of Scientific and Technological Progress (2021 Revision) that the state will encourage the application of new technology and promote trials for the application of new technology on the principles of tolerance and prudence. It emphasizes that the state should implement strategies for: (i) rejuvenating the country through science and technology; (ii) strengthening the country with talent; and (iii) driving development through innovation to support and lead economic and social development. This provides policy support and strategic guidance for AI development.

China's State Council issued a "Development Plan on the New Generation of Artificial Intelligence" in 2017.[133] The Development Plan anticipated AI as a new economic engine to provide solutions for problems such as an aging population or scarce resources, and as broadly applying in sectors such as education, medical treatment, environmental protection, city operations, and legal services. The Development Plan identified various challenges to AI development in China, such as:

- A lack of original achievements and talent;
- Large gaps with developed countries in terms of basic theories, core algorithms, key devices, high-end chips, major products or systems, materials, software, etc.;
- Absence of a legal framework; and
- Legal or ethical problems arising from the development of AI, such as the infringement of personal privacy, disruption to industry or employment structures, or impact on social governance and stability.

Following the promulgation of the Development Plan in 2017, laws, regulations, policies, and ethical rules that promote or regulate AI development were promulgated and made effective, and efforts were made to establish an AI security monitoring and evaluation system to manage any abuse of data, infringement of personal rights, breach of network security, or other potential issues.

In 2019, the Ministry of Science and Technology issued "Work Guidelines for the Construction of National Open Innovation Platforms for New Generation Artificial Intelligence."[134] The Work Guidelines designate enterprises as leaders in building

AI-related open-source platforms, promoting resource sharing, securing market-based funding, and encouraging collaboration among governments, industries, research facilities, and universities.

In 2020, to develop experimental fields for AI-related activities on a larger scale, the Ministry of Science and Technology further issued the "Guidelines for the Establishment of the National New Generation Artificial Intelligence Innovation and Development Pilot Zone."[135] The Guidelines intend to establish selected pilot zones where new laws, regulations, policies, or standards may first be tested to promote AI-related industries and infrastructure. The Guidelines list the requirements and procedures for cities seeking to serve as such pilot zones and the supporting measures that an approved city may receive, such as local government funding or resources. Thus far, the Ministry has approved 18 cities for the development of such pilot zones, including Beijing, Shanghai, Shenzhen, Guangzhou, Hangzhou, Wuhan, Suzhou, Harbin, Shenyang, and Zhengzhou. Notably, DeepSeek, a prominent AI company garnering global acclaim in 2025, is headquartered in Hangzhou, one of the designated pilot zones for AI innovation and development.

In 2022, the Ministry of Science and Technology, in collaboration with six other government agencies, issued the "Guiding Opinions on Accelerating Innovation in Specific Scenarios to Promote High-Level Application of Artificial Intelligence for High-Quality Economic Development." The Guiding Opinions encourage the exploration of new business models for AI-driven economic and social development through scenario-driven approaches. Various regions have actively responded by developing nearly a thousand application scenarios, including but not limited to smart farms, intelligent mines, smart factories, and intelligent supply chains, thereby promoting the implementation of large model applications. Government agencies in charge of specific sectors have also issued opinions or guidance to facilitate and support AI-related development in their areas, such as in forestry and grassland,[136] higher education,[137] medical software products,[138] and construction.[139]

### Guidance

Four government agencies (the National Standardization Administration, the Central Cyberspace Administration Office, the National Development and Reform Commission, and the Ministry of Science and Technology) issued "Guidelines for the Construction of the National Artificial Intelligence Industry Comprehensive Standard System" in 2024. The Guidelines set out seven main categories of various AI-related subjects for which standards are to be promulgated:

1. Basic and common standards (e.g., terminology or knowledge structure, testing, or evaluation);
2. Foundational support standards (e.g., basic data services, intelligent chips, smart sensors, computing devices, computing power centers, system software, development frameworks, and software-hardware coordination);
3. Key technology standards (e.g., machine learning, knowledge graphs, large models, natural language processing, intelligent speech, computer vision, biometric recognition, human-machine hybrid augmented intelligence, intelligent agents, swarm intelligence, cross-media intelligence, and embodied intelligence);
4. Standards for intelligent products or services, including industrial standards (e.g., intelligent robots, intelligent vehicles, intelligent mobile terminals, digital persons, and intelligent services);
5. Enabling new industrialization standards, including standards for the entire manufacturing process (e.g., research and development, design, pilot testing, production and manufacturing, marketing services, and operation management), as well as intelligent upgrade standards for key industries;
6. Industry application standards (e.g., smart cities, scientific intelligent computing, smart agriculture, smart energy, smart environmental protection, smart finance, smart logistics, smart education, smart health care, smart transportation, and smart cultural tourism); and
7. Safety and governance standards.

### Regulating AI's Ethical and Security Risks

The PRC has promulgated a series of regulations and standards to ensure AI safety and ethics by promoting responsible development and transparency, preventing illegal or harmful content, protecting user rights and privacy, and integrating ethical considerations throughout the AI life cycle, emphasizing fairness, accountability, and the prevention of bias and discrimination.

Under the Generative AI Provisions, AI service providers are held accountable as "content producers," and if any illegal content is identified among uses of these services, the services must be suspended and the incidents must be reported

to regulators. Providers are prohibited from generating content that violates PRC laws and are required to take effective measures to prevent discrimination; respect intellectual property and business ethics; safeguard trade secrets; avoid monopolization and unfair competition; avoid infringing other's rights to portraits, reputations, honors, privacy and personal information; and improve the transparency, accuracy, and reliability of generated content.

The CAC also released the Provisions on the Administration of Algorithm Recommendation for Internet Information Services ("Algorithm Provisions") on December 31, 2021, which became effective on March 1, 2022. The Algorithm Provisions regulate content output by ensuring adherence to mainstream values, establishing content review systems, and promoting transparency and user control. Providers must avoid spreading illegal or harmful information, prevent unethical behavior, and allow users to manage or disable personalized recommendations. The goal is to ensure ethical, transparent, and socially responsible algorithm recommendation services.

Jointly promulgated by the CAC, the Ministry of Industry and Information Technology ("MIIT"), and the Ministry of Public Security ("MPS"), the Provisions on the Administration of Deep Synthesis of Internet-Based Information Services regulate content output by prohibiting the creation and dissemination of illegal or harmful content, including false news. Providers must implement content review systems to filter out such information and clearly label synthetic content to prevent public confusion. These measures aim to ensure that deep synthesis services are used responsibly and ethically.

The National New Generation Artificial Intelligence Governance Specialist Committee published "Ethical Norms for the New Generation of Artificial Intelligence" in September 2021.[140] The Ethical Norms integrate ethical considerations throughout the AI life cycle; emphasize fairness, privacy protection, and accountability in AI development and use; and promote transparency, safety, and the prevention of bias and discrimination.

On ethical risks raised by AI technology, in 2021, the National Information Security Standardization Technical Committee ("TC 260") issued the "Network Security Standardization Practice Guide—Guidance for Prevention of Ethical Risks of Artificial Intelligence" ("Ethical Guidance").[141] This publication provides guidance on better addressing the ethical risks of activities such as AI research and development, design and manufacturing, and applications. The Ethical Guidance requires conducting an ethical risk analysis for an AI-related activity with respect to the following risks: (i) the ethical impact of AI, which may exceed the expectation, understanding, or control of relevant parties (such as the researcher, developer, designer, or manufacturer); (ii) inappropriate use of AI; (iii) AI infringing on basic human rights, including bodily, privacy, or property rights; (iv) AI discrimination against specific groups of people that may affect justice or equality; and (v) inappropriate conduct or unclear responsibility of relevant parties, thereby negatively impacting social trust or values or infringing on rights. In addition, the Ethical Guidance also sets out obligations on relevant parties to prevent those risks.

Subsequently, TC 260 released a series of other standards aiming to provide comprehensive guidelines for the safe and effective use of AI technologies. The mandatory national standard of "Cybersecurity Technology—Labeling Method for Content Generated by Artificial Intelligence," promulgated by TC 260 in June 2024, outlines the key requirements of explicit labeling (e.g., visible labels to indicate AI-generated text, images, audio, video) and implicit labeling (e.g., metadata), and aims to ensure transparency and traceability and prevent misuse or malicious use of AI-generated content.

| Standard | Subject | Date of Issuance |
|---|---|---|
| **AI Security Standardization White Paper (2023 Edition)** | Overview of AI security standards and guidelines | 2023 |
| **Basic Security Requirements for Generative AI Services** | Security measures for GenAI, including data and model security | 2024 |

On March 7, 2025, the CAC, MIIT, MPS, and National Radio and Television Administration released the Measures for Artificial Intelligence-Generated and Synthetic Content Labeling. The Measures mandate explicit and implicit labeling of AI-generated or synthetic content and outline obligations for service providers, platforms, and users. It is expected that clear content labeling will help improve transparency, enhance users' rights to be informed and choose, and foster the public's understanding of AI technology. Key obligations include:

- **Service Provider Obligations**. Explicit labels must be prominently added to AI-generated text, audio, images, video, or virtual scenes (e.g., text prompts, symbols, audio cues, or watermarks) and remain visible during downloading or sharing. Implicit labels, i.e., technical metadata such as creator details or content ID, must be embedded. Digital watermarks are also encouraged.
- **Platform Obligations**. Distribution platforms must require internet application service providers to indicate whether they offer AI-generated or synthetic services. If so, distribution platforms are required to verify relevant labeling of content.
- **User Obligations**. Users must label AI-generated or synthetic content when publishing it to online information dissemination services. Users are prohibited from deleting, altering, forging, or concealing the required labels of generative or synthetic content, and from using improper labeling methods that harm others' legitimate rights or interests.

### Data Annotation

Under the Generative AI Provisions, GenAI service providers are required to tag content generated by their AI systems. During the research and development stage, these providers must establish clear, specific, and practical labeling rules for the training data. Additionally, they must conduct quality assessments of data labeling and perform sample verification to ensure the accuracy of labeled content.

### User Protection

AI service providers are also required to take effective measures to prevent minor users from becoming excessively reliant on or addicted to GenAI services.

## JAPAN

As a result of continued discussion as described below, Japan has recently shifted from a "soft law" approach to a legally binding approach to regulating AI's use and development—though still not as hard and comprehensive as the EU approach—with the intention of leaving AI's use and development undeterred.

Japan initially provided only non-legally binding guidelines. On July 9, 2021, METI published a report titled "AI Governance in Japan ver. 1.1" ("AI Governance Report").[142] Following a review of various regulatory approaches taken in other jurisdictions, the AI Governance Report concluded that for Japan, a desirable AI governance approach would not establish legally binding comprehensive laws and regulations. Rather, Japan would provide guidelines setting out various risk-based options and practical examples to fill in the gaps and achieve the goals of the parties concerned. Based on the AI Governance Report's recommended approach, on January 28, 2022, METI published "Governance Guidelines for Implementation of AI Principles Ver. 1.1" ("AI Governance Guidelines").[143]

Separately, MIC, through the Conference toward AI Network Society, published "Draft AI R&D Guidelines for International Discussions" on July 28, 2017,[144] and "AI Utilization Guidelines Practical Reference for AI Utilization" on August 9, 2019.[145] According to its 2022 Annual Report,[146] the Conference is considering the review and amendment of these guidelines in light of recent developments in these areas.

On April 19, 2024, METI and MIC jointly published "AI Guidelines for Business Ver 1.0" ("AI Guidelines for Business").[147] The AI Guidelines for Business were newly established to help business operators in collaboratively addressing the social implementation and governance of AI. They integrate and adapt the three existing guidelines above: the AI Governance Guidelines, Draft AI R&D Guidelines for International Discussions, and AI Utilization Guidelines Practical Reference for AI Utilization.

The AI Guidelines for Business reflect recent advancements in AI technologies as well as domestic and international

discussions regarding the social implementation of AI. They are designed to replace the previous guidelines, providing a unified framework to help business operators understand the guiding principles that lead to the safe and secure use of AI.

In parallel, given the rise of international movement toward stricter legal regulation of AI utilization and development, the Cabinet Office discussed how to regulate AI, including whether new legal restrictions were necessary. These discussions aimed to balance risk management with fostering innovation while ensuring alignment with the systems of other countries. As a result, on February 28, 2025, the Act on Promotion of Research, Development and Utilization of AI-related Technologies ("AI Bill") was approved by the Cabinet and submitted to the Diet. The AI Bill was enacted on May 28, 2025, and it is the first law regulating AI in Japan. However, this is still a basic law that provides only foundational principles and general responsibilities of each player—namely, national and local governments, research and development organizations, and business entities as AI users—and thus provides no penalties to be imposed on businesses for violation or misuse of AI technologies.

### AUSTRALIA

#### Existing Legislative Schemes

Many existing legislative regimes stand to capture, regulate, and prohibit AI uses, particularly general criminal provisions. The Australian federal government has specifically cautioned about the potential for harmful AI outputs to violate the *Australian Consumer Law*, including product liability laws, such as where a defect in an output causes a cybersecurity risk, where outputs are misleading or deceptive, or where there is a failure to disclose when AI is being used in a service.

#### Novel Legislative Reforms

The regulation of deepfake sexual content represents the first legislative act in Australia aimed directly at prohibiting an AI use. In the second half of 2024, the Criminal Code Amendment (Deepfake Sexual Material) Act 2024 (Cth) was enacted. The act bans the creation and nonconsensual distribution of deepfake pornography, criminalizing the transmission of sexual material of another person, irrespective of whether the material was created or altered by technology, and makes such conduct punishable by up to six years of imprisonment.

## AI LIABILITY

**Issues.** Notwithstanding any market access limitations, AI's rapid emergence and its distinctive characteristics (such as opacity, unpredictability, connectivity, complexity, and autonomy) have triggered calls for establishing specific liability rules for material and immaterial harm "caused by" AI. One of the challenges raised by AI is the allocation of liability, since damage might be traced back to neither human error nor to a product defect and can derive from its above-referred particularities:

- Machine learning enables digital systems to learn autonomously through experience and by using data, which are not all in the hands of the initial programmer.
- The opacity of AI systems may raise difficulties in understanding how such systems produce a certain output.
- With the internet of things in industrial production, product defects may be due to the connectivity of an increasing number of robots and devices.

In cases where AI "causes" damage, the question therefore arises as to who would be the addressee of a damage claim. The answer is not so simple, as many addressees could be considered, such as the algorithm's creator, the software producer, the database owner, the connectivity provider, the AI system owner, the AI user, etc. The requirement to demonstrate a causal link raises another challenge caused by the complexity of AI systems and poses a great burden on the injured party. Finally, fulfilling the condition of fault may be difficult to prove in relation to AI systems.

As a result, authorities across the globe are considering introducing specific liability regimes for AI damages, such as joint and several liability, strict liability (without fault), and others.

### EUROPEAN UNION

#### Current Legislation

EU Member States essentially oversee liability regimes. However, the European Union has recently been working toward greater harmonization among these regimes. This effort includes the newly adopted Revised Product Liability Directive,[148] which repeals and replaces the former Product Liability Directive.[149]

### Specific Liability Rules for AI

The EU AI strategy (and its annexes[150]), as well as related expert reports[151] and communications,[152] concluded that further harmonization of liability rules was required to address AI's specificities. Following a consultation in October 2021,[153] the European Commission published the Revised Product Liability Directive.

The Revised Product Liability Directive entered into force on December 8, 2024. Member States will have two years—until December 9, 2026—to transpose the directive into their national laws.[154]

The Revised Product Liability Directive aims at modernizing the EU framework on manufacturers' and other economic operators' civil liability for defective products and includes the following reforms:

- Extending the definition of "product" to enable strict liability rules to cover intangible products such as software, including AI systems, although the EU legislator explicitly excludes from the text's scope any free and open-source software developed or supplied outside the course of a commercial activity.
- Broadening the scope of damages to new types of damages, such as loss of data, provided that such data is not used for professional purposes.
- Widening the strict liability regime for importers to include distributors, such as online intermediaries (online market places), where consumers cannot identify the producer. Thus, for products originating from outside the European Union, both online intermediaries and importers of physical products are to be subject to strict liability rules.
- Extending the notion of "defect" to cover defective refurbished, remanufactured, or substantially modified products and defective spare parts that cause damage. This expansion addresses the fact that AI systems continuously learn and develop while operating, and are continuously updated with new data and software.
- Exempting manufacturers from liability if the state of scientific and technical knowledge at the time the product was manufactured made it impossible to detect the defect, the so-called "state of art defense." However, Member States have the discretion to exclude this exemption when transposing the directive into national law.
- Facilitating claims to compensation by requiring manufacturers to disclose necessary information in court, including in collective claims, and by easing the burden of proof for victims in more complex cases, as in those involving AI-enabled products.

The Revised Product Liability Directive harmonizes liability rules across Member States and thus reduces legal fragmentation. However, such harmonization is limited to tort law, while national laws continue to govern contractual liability (including liability exemptions, etc.).

## UNITED KINGDOM

The United Kingdom does not have a single statute that outlines an approach to AI liability. However, it is anticipated that regulators such as the CMA, FCA, ICO, and Ofcom will be closely monitoring AI developments in line with their wider enforcement powers. For example, the CMA recently acquired wider direct enforcement powers though the Digital Markets, Competition and Consumers Act 2024. This enables the CMA to directly enforce consumer protection law against infringing parties, with significant penalties for noncompliance. The CMA released a draft guidance note on its approach to enforcement in December 2024,[155] which provides a summary of the CMA's consumer investigatory and enforcement powers and functions.

Although AI patents have been subject to some litigation, the use and regulation of AI has not yet been meaningfully litigated in the United Kingdom. At the time of writing, only one case has reached UK courts: *Getty Images (US) Inc & Ors v Stability AI Ltd* [2023] EWHC 3090 (Ch).

Getty Images' claim is in relation to Stability AI's deep-learning model, which is capable of generating "synthetic image outputs in response to user commands." Getty alleges that Stability AI used its copyrighted images without consent to train the AI model, thereby unlawfully reproducing Getty's copyright, and further argues that certain synthetic image outputs of Stability AI's model infringe Getty's copyright. The causes of action that Getty relies on are copyright infringement, database rights infringement, trademark infringement, and passing off. The copyright infringement claims are further divided into the following sections: (i) the "Training and Development Claim"; (ii) the "Secondary Infringement Claim"; and (iii) the "Output Claim," which concerns the generation of images from either text, images, or a combination of text and image prompts. The High Court refused to grant summary judgment on the case in 2023, and the case went to trial in June 2025. It could be a considerable time until we receive a judgment on this pivotal decision, which is likely to face appeal in the UK courts and thus further delay.

## UNITED STATES

The United States does not have a comprehensive approach to AI liability at either the national or state level. At the state level, legislatures are seeking to update their general tort laws to cover certain AI-based damages. For example, many states have already passed legislation related to autonomous vehicles to update existing damages laws.[156] To address AI-based harms more broadly, further legislation could come in the form of updating existing product liability laws. Given product liability law's history of adapting to new technologies, advocates have argued it is the best vehicle to address the potential harms that may result from AI products. Even without AI-specific updates to product liability or tort laws, developers and deployers of AI systems that adhere to industry custom and standards will be in a better position to defend against general negligence claims than those who fail to do so.

The absence of clear liability for harm caused by AI systems has prompted some states to create frameworks to address these gaps in accountability. In March 2024, Utah passed the Utah Artificial Intelligence Policy Act, which, effective May 2024, requires businesses operating within the state that utilize GenAI to disclose such usage when prompted by a customer inquiry. Notably, the law prohibits companies from escaping liability by blaming consumer protection violations on the GenAI systems they deploy. Further, criminal liability may attach if a person commits an offense with the aid of GenAI, or intentionally prompts a GenAI tool to commit a criminal offense.[157]

Aside from liability for harms caused by AI, publicly traded companies may face potential liability for making inaccurate or misleading disclosures about their use of AI. Companies must be careful not to exaggerate or misstate how they are using AI in their businesses, a practice labeled "AI washing" by the SEC.[158] Agency guidance encourages companies to avoid boilerplate disclosures and seek to provide particular information on how and where a company is using AI.[159]

Lastly, the rise of AI—particularly GenAI—calls into question the scope of immunity under Section 230 of the Communications Decency Act, which provides immunity to internet platforms for most content posted by third-party users. Without clarifying legislation, courts will need to determine on a case-by-case basis whether an AI-generated output is attributable to the platform providing the interactive computer service or to the user.

### Infringement Liability

GenAI also raises questions that pressure-test the contours of intellectual property law.

Numerous lawsuits involving AI and infringement liability are pending in federal district courts in the United States, including cases involving AI patents, alleged copyright infringement by AI training models and/or GenAI outputs, and trade secret misappropriation. There are more than a dozen significant lawsuits currently pending (including the United States counterpart to the UK Getty–Stability AI case referenced above), in which the plaintiffs have alleged that their copyrighted works were used as part of the training data for GenAI tools without authorization, and that this use constitutes copyright infringement. Some plaintiffs have alleged copyright infringement in the outputs of GenAI tools—that users can prompt certain tools to produce infringing outputs that are substitutes of the

original copyrighted work. A key defense in these cases is fair use—i.e., whether using copyrighted works to train AI models constitutes fair use.

In a recent federal case that was touted as the first case to substantively resolve the fair-use question in the context of AI, the court granted summary judgment to a copyright owner. The court held that the use of copyrighted materials to train a competing AI tool is not fair use under the Copyright Act.[160] However, the court was careful to parse through the particular facts at issue in that case and, among other things, noted that the case did not involve GenAI (whereas many of the other pending AI/copyright cases do involve GenAI tools where the defendants will emphasize the "transformative" nature of the tools). As fair use is a notoriously fact- and context-specific inquiry, the outcomes in these cases may vary. This type of litigation in the United States is evolving rapidly.

In addition, AI may reshape the contours of the safe harbor under the Digital Millenium Copyright Act ("DMCA"), which protects digital copyrights and establishes a system for online service providers to address copyright infringement. For example, it remains unclear whether providers of AI systems are considered qualifying service providers under the DMCA for purposes of the liability safe harbor. Considering ongoing litigation on this issue, courts and lawmakers are poised to reevaluate the scope of safe harbor protections.

Both U.S. courts and federal agencies have concluded that the human authorship and human inventorship requirements under U.S. copyright and patent law are in full force. Thus, works that are generated by GenAI tools without sufficient human participation will not satisfy those requirements. In the 2022 case *Thaler v. Vidal*, the Federal Circuit concluded that a patent is invalid if the invention was not conceived by a natural person.[161] The U.S. Patent and Trademark Office later issued guidance indicating that patent protection may remain available provided a natural person makes a "significant contribution" to the invention.[162]

Similarly in the copyright context, in the 2025 decision in *Thaler v. Perlmutter*, the U.S. Court of Appeals for the D.C. Circuit affirmed the denial of a copyright application where the "author" was identified as an AI tool, finding that only human beings can be authors under U.S. copyright law.[163] The U.S. Copyright Office has offered guidance to explain that while a human author may be assisted by technology (including AI) to create a work, the human authorship requirement is indeed fundamental to U.S. copyright law. A creative process satisfies copyright's human authorship requirement only if a natural person maintains sufficient control over the expressive elements of the work.[164]

In addition to providing guidance on the copyrightability of AI outputs, the U.S. Copyright Office has also expressed concerns about unauthorized digital replicas, or "deepfakes." The office recommended that Congress establish a federal law that protects individuals from deepfakes during their lifetime.[165] The Copyright Office recently (in May 2025) issued a "prepublication" version of a report on training AI models using copyrighted works, offering its view that not all forms of such training will constitute "fair use" but noting that the fair use analysis is highly fact-specific and must be resolved on a case-by-case basis.[166] The Copyright Office is expected to provide additional guidance on AI and copyright this year, with a focus on potential liability for outputs that infringe copyrights and transparency requirements.

## CHINA

### Personal Rights

At present, while China does not have a comprehensive approach to AI liability, AI providers and users are subject to liability. At the highest judicial levels, Chinese courts are taking interest in safeguarding individual rights against AI-related infringements. For example, in April 2022, the Supreme People's Court identified a number of "model" civil cases on personality rights issued by lower courts in China. These included a ruling by the Beijing Internet Court, which found that AI software infringed personality rights by using the portrait of a natural person without the person's consent.[167] The AI software at issue allowed users to build an AI virtual character using the plaintiff's name, portrait, and character traits, and to interact with it. The court ruled that the software provider, by designing this function and algorithm, in fact encouraged users to use the plaintiff's information in this way. Therefore, it was no longer a neutral technology provider and infringed the plaintiff's rights to name, portrait, and dignity. This case

involved a detailed exploration of standards for assessing AI algorithms and applications and highlights the court's view of the significance of protecting personality rights in the AI age.

In 2023, the Chinese judicial practice rendered further decisions in favor of individuals, based on the protection of their personal rights, including the right to voice,[168] against infringement by products and activities related to GenAI. Notably, these cases were not appealed to higher courts or the Supreme People's Court of China. Their decisions remain controversial and are often disputed by other practitioners, leaving the future of judicial enforcement uncertain.

## JAPAN

Japan has not yet enacted any specific rules to address AI liability issues. Therefore, AI liability is governed by the current civil contractual or tort liability regimes under the Civil Code of Japan (Act No. 89 of April 27, 1896, as amended)[169] and the Product Liability Act (Act No. 85 of July 1, 1994).[170]

Like the current EU Product Liability Directive, Japan's current Product Liability Act covers only a defect of a "product" that is movable property. Therefore, if AI is installed in and constitutes a part of a certain device, the manufacturer of such device could be subject to product liability. However, if AI is not installed in a device and is merely a program, it cannot be construed as a movable object, and thus is not a product. Therefore, liability claims cannot be made against a programmer of AI under the Product Liability Act. The notion of defect[171] and the appropriate burden of proof, as discussed in the proposed revision of the EU Product Liability Directive, would also need to be examined under the Product Liability Act.

Like courts in the United States, Japanese courts have concluded that patents may be issued for the inventions of a natural person only. In the absence of a named human inventor, an invention is not entitled to patent protection.[172]

## AUSTRALIA

### Existing Liability Regimes

The Australian federal government has forecasted the possibility of liability for the outputs of AI under existing regimes in several areas of law, notably including:[173]

- Negligence law, where an organization fails to exercise the standard of care of a reasonable person to avoid foreseeable harm to persons to whom it owes a duty of care, and causes harm;
- Criminal law, including indirectly where an output of an AI aids or abets the commission of a crime;
- The Online Safety Act 2021 (Cth), where outputs produce restricted, harmful, or otherwise illegal online content;
- Defamation law, where AI outputs are defamatory and the organization participated in the process of making the defamatory material (such as through making the tool available for training);
- Antidiscrimination law, where outputs exclude or disproportionately affect an individual or group on the basis of a protected attribute; and
- Corporate governance laws, in particular, directors' duties to assess and govern risks to an organization that is deploying or designing AI.

The Australian Consumer Law has already been applied to impose penalties against the deployer of an algorithm that produced outputs that the federal court ultimately held were misleading. In 2020, the case of *Australian Competition and Consumer Commission v Trivago N. V.*[174] saw Trivago fined approximately A$45 million in the Federal Court of Australia for its aggregation of deals offered by online hotel booking sites in a way which, using an AI-based algorithm, showed "Top Position Offers" to consumers—offers that were in fact higher-priced rooms rather than lower-priced alternatives.

### Novel Legislative Reforms

The Privacy Act Amendment Bill additionally creates a new liability framework applicable to AI developers and deployers: a statutory tort applying to breaches of privacy, creating an

actionable right to seek redress for breaches of privacy and misuse of information where the individual had a reasonable expectation of privacy. A claim needs to satisfy a public interest test in order to succeed, and will also be subject to specific exemptions from liability, including for journalism.

In a discussion paper released on October 15, 2024, reforms to the Australian Consumer Law to address the use of AI in the marketplace were proposed. The Australian federal government sought engagement on ways to protect consumers who use AI and support the safe and responsible use of AI by business, including questions of the application of existing consumer guarantees and access to remedies. The federal government flagged specific prohibitions on false and misleading representations in relation to AI, specific consumer guarantees regarding AI, AI product safety standards, and new unfair contract terms specific to AI. Consultation for this review closed on November 12, 2024. It remains to be seen what changes will be proposed following this review.

## CONCLUSION—KEY CONSIDERATIONS FOR THE PRIVATE SECTOR

For businesses, innovative development and deployment of AI pose tremendous opportunities but also legal risks. Navigating these opportunities and risks will require knowledge of the legal implications of and a strategic approach to the evolving legal issues presented. While each situation, product, and service will pose different questions, below are some general recommendations to consider in managing AI risk in the current landscape.

**Keep Abreast of Global AI Regulatory Trends and Developments and Specific Developments in Key Geographies Relevant to Your Business.** When developing new AI systems, companies should anticipate constraints that existing or upcoming regulation may impose, including in terms of conditional market access, increased liability, or data usage. Companies should expect to have to adapt to increasing constraints as more regulations are imposed and, in some legal systems, as new causes of action are created or recognized.

The European Union is the frontrunner in terms of setting the regulatory constraints, with expected regulations covering: (i) the marketing and use of AI systems; (ii) data access; and (iii) AI liability. This framework may become a blueprint for regulation in some other countries (or by subnational state or local authorities), as the GDPR did for privacy regulation.

In the United States, the patchwork approach to AI regulation has meaningful implications for companies, whether well-established with AI-based technologies or those newly adopting or developing those technologies. Depending on its area of business, a company may find itself entering a highly regulated space in which established guidelines govern acceptable practices, or a company may have little oversight and be left to develop best practices on its own. However, the establishment of the NAIAC indicates the growing interest in taking a more comprehensive approach to AI technologies at the federal level.

**Consider Data Collection Risks and Opportunities.** When deploying AI, companies should consider the risk and opportunities of lock-in effects. Companies should consider their strategies to gather relevant and sufficient data to support their AI-based products and services. The rising importance of data-sharing and pooling arrangements, as well as data access, portability, and privacy issues, may create regulatory concerns. In this regard, they should consider opportunities brought by existing and new regulations in terms of access and portability of data, which may facilitate access to competitors' data or to data owned by third parties that relate to its own activities. Companies should review data-pooling agreements with their competitors under competition and privacy laws.

**Maintain Privacy Practices Where AI Implicates Personal Data.** AI systems using personal data call for specific attention, as impact to individuals is a universal focus of evolving AI regulation, and the handling and processing of personal information already is governed independently by privacy legislation in most jurisdictions. The EU obligation to conduct impact assessments should be considered. In the United States, companies can expect ongoing debate on the implementation of a national data privacy regulation like the GDPR and both federal and state AI-specific privacy legislation. Risk will increase with growing regulatory complexity and potential inconsistency.


**Monitor Data Flows.** Several regulations, like the GDPR in the European Union, or the Measures for the Security Assessment of Outbound Data Transfer in China, may constrain the transfer of data or algorithms between jurisdictions. Such considerations can apply to transfers of data within a company, or to collaborative software development projects in which code is transferred between or accessible by personnel in multiple jurisdictions. For example, the United States and China have each signaled an intention to restrict exports of certain high-value AI technologies to each other (although on December 21, 2023, China newly revised and lessened the export restriction of speech synthesis and AI interaction interface technologies to those specifically for Chinese and minority languages[175]). Companies should map the data flows triggered by AI use and assess their compliance.

**Put in Place an Internal Structure to Limit the Risks of Discrimination and Bias and Confirm that AI Systems Do Not Inadvertently Create Imbalanced Outcomes.** Specific attention should be given to risks of biases triggered or amplified by AI usage, including the potential for so-called "reverse discrimination." It has become increasingly clear that, regardless of the field, governments are motivated to focus on ensuring AI technologies are not used in a discriminatory manner or result in discriminatory practices. Given that AI technologies are iterative and learning-based, a company should consult with experts to confirm that training datasets are free from biases from the outset. The regulatory agencies that have commented on the matter have made clear that a lack of intent is not exculpatory should use of an AI system result in discriminatory practices. Internal audits should be considered to map the AI used within a company and assess the need to establish ethics principles and governance (ethical board, etc.) to control such use. Additionally, checks should be in place designed to guard against new forms of bias or imbalanced outcomes resulting from efforts to reduce discrimination, to maintain fairness and equity across all dimensions.

**Manage Liability Risks.** Navigating multiple increasingly prescriptive, and occasionally conflicting, regulatory regimes and liability concepts will pose a growing array of challenges for companies. Company liability and the service-level landscape warrant careful assessment to minimize the exposure to claims based on asserted data protection lapses, malfunction, or bias (e.g., race or gender related). Using AI systems, even when off-the-shelf, can raise specialized questions or concerns in certain contexts, such as in relation to employment matters or public safety. Regulatory compliance should be monitored, and licensing contracts relating to software or data call for careful review to properly allocate liability.

**Protect Your AI-Related IP Rights.** AI providers and users generally want to protect their respective IP rights and business data, which may raise more complexities if involving AI. For businesses with a multijurisdictional corporate structure, employee or contractor base, or pool of customers or vendors, a key concern will be to protect IP and provide for regulatory compliance in multiple jurisdictions whose governments may approach AI and data regulatory issues in distinctly different manners—and that may restrict the export of data or AI algorithms to each other.

**Integrate AI-Specific Aspects in M&A Transactions.** When conducting an M&A transaction, in particular when an AI system is a key production or a key target asset, it may be advisable to integrate specific questions within the due diligence to enable identification of specific risks incurred by AI systems, e.g., in terms of expected restriction to the market potential of an AI system, the license contracts used for AI systems, whether adequate IP protections have been secured in relevant jurisdictions, the data to be run on AI systems, etc. In addition, the acquisition of AI assets can trigger particular attention under foreign direct investments *ex ante* control, like CFIUS, which may delay or even, in some cases, prevent the transaction. In each case, attention to these issues in advance can help the parties apportion risk and avoid subsequent delays to closing or post-closing integration.

**Manage AI Procurement and Vendors.** It will also be crucial to conduct thorough due diligence on AI vendors, including their data-security practices, compliance with legal requirements, and ethical standards. In addition, it will be necessary or prudent to include in AI contracts appropriate clauses regarding data privacy, security, liability, and intellectual property. With regard to vendor management, companies should consider establishing a process for managing AI vendors, including ongoing monitoring of their performance and compliance with contractual obligations.

Legal frameworks are still developing and are subject to change—along with the technology itself, which continues to evolve rapidly as R&D efforts progress and a wider range of organizations focus on adapting AI to their objectives. The law is now sufficiently developed and the use of AI so pervasive, however, that AI presents a meaningful risk for virtually all companies across industries and jurisdictions.

## LAWYER CONTACTS

This *White Paper* serves as a starting point for consideration of issues that will in many cases warrant fact-specific review, and we encourage readers to contact the following Jones Day lawyers with questions.


**Karen P. Hewitt**
San Diego
+1.858.314.1119
kphewitt@jonesday.com

**Mauricio F. Paez**
New York
+1.212.326.7889
mfpaez@jonesday.com

**Emily J. Tait**
Detroit
+1.313.230.7920
etait@jonesday.com

**Jeffrey J. Jones**
Detroit/Columbus
+1.313.230.7950/+1.614.281.3950
jjjones@jonesday.com

**Jörg Hladjk**
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

**Undine von Diemar**
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

**Haifeng Huang**
Hong Kong/Beijing
+852.3189.7288/+86.10.5866.1111
hfhuang@jonesday.com

**Richard Hoad**
Melbourne
+61.3.9101.6800
rhoad@jonesday.com

*Associates James M. Twieg, Theodora Oh, Jennifer Lin, Sophie Burgess, Alexander Wagner, and Giorgi Gugenishvili contributed to this* White Paper.

## ENDNOTES

1 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (Apr. 27, 2016) (General Data Protection Regulation).

2 EU Product Liability Directive 2024/2853 on liability for defective products and repealing Council Directive 85/374/EEC (Oct. 23, 2024).

3 Eur. Parliament, Panel for the Future of Sci. & Tech., The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence (June 2020).

4 Opinion 28/2024 on certain data-protection aspects related to the processing of personal data in the context of AI models (Dec. 18, 2024).

5 Eur. Data Prot. Bd., EDPB Stakeholder Event AI Models (Nov. 5, 2024).

6 European Data Protection Board, Guidelines 02/2025 (June 20, 2025).

7 Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union (Nov. 28, 2018).

8 Directive (EU) 2019/1024 on open data and the reuse of public-sector information (June 20, 2019) (recast). As an EU directive (unlike a directly applicable EU regulation), the Open Data Directive required Member State transposition into national laws by July 17, 2021.

9 Eur. Comm'n, Communication from the Commission, A European Strategy for Data (Feb. 19, 2020).

10 Regulation EU 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (May 30, 2022) (Data Governance Act).

11 *See* Jones Day *Alert*, EU Releases Data Act to Facilitate Access and Use of Data (Jan. 8, 2024); Jones Day *Alert*, European Commission Proposes Legislation Facilitating Data Access and Sharing (Feb. 23, 2022); Regulation (EU) 2023/2854 on harmonized rules on fair access to and use of data (Dec. 13, 2023).

12 Regulation (EU) 2024/1689, Art. 53.

13 Directive (EU) 2015/2366 on payment services in the internal market (Nov. 25, 2015). *See also* Proposal for a new (EU) Directive on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC (June 28, 2023); Eur. Data Prot. Bd., Guidelines 06/2020 on the interplay of the Second Payment Directive and the GDPR (Dec. 15, 2020).

14 Directive (EU) 2019/944 on common rules for the internal market for electricity (June 5, 2019); Directive (EU) 2024/1788 on common rules for the internal markets for renewable gas, natural gas, and hydrogen (June 13, 2024). On June 13, 2024, Regulation 2024/1747 and Directive 2024/1711 of the European Parliament and Council were officially adopted. The main purpose of the new Regulation and Directive is to amend Regulation 2019/943 and Directive 2019/944 in order to improve the design of the Union's electricity market. Some measures were included in a consolidated version of the Electricity Regulation and entered into force on July 17, 2024. Other measures were included in a consolidated version of the Electricity Directive to be transposed by Member States by January 17, 2025.

15 Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (May 20, 2019) (Digital Content Directive).

16 Regulation (EU) 2018/858 amending Regulation (EU) 2007/715 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components, and separate technical units intended for such vehicles (May 30, 2018).

17 Directive (EU) 2023/2661 amending Directive (EU) 2010/40 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (Nov. 22, 2023).

18 The Commission launched a public consultation in March 2022 on the sharing of vehicle-generated data (closed on August 2, 2022). Such vehicle-generated data will be subject to the EU Data Act. In September 2025, the Commission published guidance tailored to automotive stakeholders on how address vehicle-generated data under this new regulation.

19 Regulation (EU) 2023/1804 on the deployment of alternative fuels infrastructure (Sept. 13, 2023).

20 Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Sept. 14, 2022). *See* Jones Day *White Paper*, Digital Markets Act: European Union Adopts New "Competition" Regulations for Certain Digital Platforms (Aug. 1, 2022).

21 Eur. Comm'n, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (May 3, 2022).

22 Eur. Comm'n, European Health Data Space; Eur. Parliament, Provisional Agreement Resulting from Interinstitutional Negotiations, Proposal for a Regulation the European Parliament and the Council of the European Union on European Health Data Space (Mar. 22, 2024).

23 Regulation (EU) 2025/327 on the European Health Data Space (Feb. 11, 2025).

24 Regulation (EU) 2025/1183, Arts. 42–47.

25 In the European Union, "entry into force" is the date of the legal existence of a regulation or directive. Directives impose an "implementation date" for transposition into Member State law. In general, Member States should have transposed the directive into national law within the time frame specified by the directive, at which point the transposition law applies in the respective Member State. Regulations, on the other hand, do not require transposition and apply directly across Member States from the day they become "applicable."

26 *See* Eur. Comm'n, Communication from the Commission, Guidelines on the Applicability of Article 101 of the Treaty on the Functioning of the European Union to Horizontal Co-operation Agreements § 418 (June 1, 2023).

27 *See, e.g.*, *Insurance Ireland: Insurance Claims Database and Conditions of Access* (Case AT.40511) Comm'n Decision (June 30, 2022) (where the European Commission has made commitments offered by Insurance Ireland, an association of Irish insurers, legally binding under EU antitrust rules. Accordingly, Insurance Ireland must ensure fair and nondiscriminatory access to its Insurance Link information exchange system).

28 *See*, *e.g.*, *Reuters Instrument Codes* (Case AT.39654) Comm'n Decision (Dec. 20, 2012) (where the European Commission has made commitments offered by Thomson Reuters to create a new license allowing customers, for a monthly fee, to use Reuters Instrument Codes ("RICs") for data sourced from Thomson Reuters' competitors).

29 For example, the Open Data Directive limits the exceptions allowing public bodies to charge more than the marginal costs of dissemination for the reuse of their data and strengthens the transparency requirements for public–private agreements involving public-sector information.

30 Eur. Comm'n, Press Release, Commission calls on Member States to review outbound investments and assess risks to economic security (Jan. 15, 2025); *see also*, Jones Day *Commentary*, The Rise of Outbound Investment Screening: The U.S. and EU Initiate Measures (Feb. 10, 2025).

31 *See* Jones Day *Commentary*, The Rise of Outbound Investment Screening: The U.S. and EU Initiate Measures (Feb. 10, 2025).

32 Eur. Comm'n, Recommendation (EU) 2025/63 (Jan. 2025) (on reviewing outbound investments in technology areas critical for the economic security of the Union).

33 Info. Comm'r's Off., Regulating AI: The ICO's Strategic Approach (Apr. 2024).

34 *See, e.g.*, Info. Comm'r's Off., AI Tools in Recruitment (Nov. 2024); Generative AI: Eight Questions that Developers and Users Need to Ask (Apr. 3, 2023); Guidance on AI and Data Protection (Mar. 15, 2023).

35 Info. Comm'r's Off., Generative AI First Call for Evidence: The Lawful Basis for Web Scraping to Train Generative AI Models.

36 Dep't for Sci., Innovation & Tech., Cyber Security and Resilience Bill (Sept. 30, 2024).

37 *See* Jones Day *Alert*, FDA's Final Guidance Provides Practical Approach for AI-Enabled Devices Implementing Post-Market Modifications (Dec. 27, 2024).

38 *See* Jones Day *Commentary*, Executive Order Limits Sale or Transfer of Personal Data to Certain Countries (Mar. 1, 2024).

39 *See* Jones Day *Commentary*, The Rise of Outbound Investment Screening: The U.S. and EU Initiate Measures (Feb. 10, 2025).

40 *See* Jones Day *Alert*, New Export Control Rule Regulates Global Diffusion of Artificial Intelligence (Feb. 5, 2025).

41 White House, Winning the Race: America's AI Action Plan (July 2025).

42 Executive Order 14319, Preventing Woke AI in the Federal Government (July 23, 2025).

43 Executive Order 14318, Accelerating Federal Permitting of Data Center Infrastructure (July 23, 2025).

44 Executive Order 14320, Promoting the Export of the American AI Technology Stack (July 23, 2025).

45 AI Action Plan, *supra* note 41, at 3.

46 See NIST-AI-600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (July 2024).

47 AI Action Plan, *supra* note 41, at 4.

48 *See* Jones Day *Newsletter*, Vital Signs: Digital Health Law Update | Fall-Winter 2024 (Dec. 16, 2024).

49 *See* International Association of Privacy Professionals, U.S. State Privacy Legislation Tracker (Mar. 3, 2025).

50 *See* Saryu Nayyar, Is It Time For A U.S. Version Of GDPR?, Forbes Technology Council (Feb. 1, 2022).

51 Nat'l People's Cong., Personal Information Protection Law of the People's Republic of China (available in Chinese only) [hereinafter "PIPL"]. *See also* Jones Day *Commentary*, China to Start Implementing Restrictions on Cross-Border Transfers of Personal Information (Aug. 2, 2022).

52 PIPL, art. 13.

53 PIPL, art. 24.

54 Cyberspace Admin. of China, Measures for the Security Assessment of Outbound Data Transfer (2022), art. 4 (July 7, 2022).

55 PRC Antitrust Law, art. 9 (amended 2022) (available in Chinese only).

56 Interim Provisions on Management of Generative Artificial Intelligence Services, effective Aug. 15, 2023 (available in Chinese only).

57 *See* Measures for Labeling of AI-Generated Synthetic Content, Mar. 14, 2025 (available in Chinese only).

58 *See* Basic Security Requirements for Generative Artificial Intelligence Services, promulgated on Feb. 20, 2024 (available in Chinese only).

59 *See* The Provisions on Regulating and Promoting Cross-border Data Flow, promulgated and effective on Mar. 22, 2024 (available in Chinese only).

60 *See* China (Beijing) Free Trade Zone Data Export Management List (Negative List) (2024 Edition) (available in Chinese only).

61 *See* Regulation on Lin-Gang Special Area of China (Shanghai) Pilot Free Trade Zone (2022); Shanghai Data Regulation (2021).

62 Significant amendments to the APPI were made in 2020 and 2021. The 2020 amendment in its entirety and the 2021 amendment partially took effect on Apr. 1, 2022. The 2021 amendment fully took effect on April 1, 2023. An English translation is available for the 2021 amendment of the APPI.

63 APPI, art. 21, para. 1.

64 APPI, art. 27, para. 1.

65 APPI, art. 28, para 1.

66 APPI art. 28, para. 2; APPI implementation regulation, art. 17, para. 2.

67 "Anonymously processed information" is information relating to an individual that is processed such that a specific individual cannot be identified and the original form of the personal information cannot be restored, APPI art. 2, para. 6.

68 APPI art. 20, para. 2.

69 APPI art. 27, para. 2.

70 Act on Anonymized Medical Data and Pseudonymized Medical Data That Are Meant to Contribute to Research and Development in the Medical Field, Act No. 28 (2017) (available in Japanese only).

71 Next Generation Medical Infrastructure Act, art. 52 (May 2017).

72 *Id.* art. 57.

73 *Id.* art. 36.

74 Study Group on Data and Competition Policy (available in Japanese only).

75 Act on Prohibition of Private Monopolization and Maintenance of Fair Trade, Act. No. 54 (Apr. 14, 1947).

76 *See, e.g.*, Austl. Hum. Rts. Comm'n, Australia Needs AI Regulation (Aug. 16, 2023).

77 *Comm'r Pats. v. Thaler* [2022] FCAFC 62.

78 *Austl. Competition & Consumer Comm'n v. Trivago N.V.* [2020] FCA 16.

79 Privacy and Other Legislation Amendment Bill 2024. Children's Online Privacy Code to be developed and registered by December 10, 2026.

80 *See, e.g.*, *Fortune*, Facial Recognition Firm Clearview Fined €30.5 Million and Banned from Using "Invasive" AI in the Netherlands (Sept. 3, 2024); Clearview AI, Clearview AI Settles ACLU Illinois Lawsuit Confirming Continuity of Business Supporting Public Safety (May 12, 2022).

81 Eur. Comm'n, Communication from the Commission, Artificial Intelligence for Europe, COM/2018/237 final (Apr. 26, 2018).

82 Eur. Comm'n, Communication from the Commission, Fostering a European Approach to Artificial Intelligence, COM/2021/205 final (Apr. 21, 2021).

83 Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence (June 13, 2024).

84 Regulation (EU) 2023/988 on general product safety (May 10, 2023).

85 Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Oct. 23, 2024).

86 *See also,* Jones Day *Commentary* Regulating Artificial Intelligence: European Commission Launches Proposals (Apr. 29, 2021); Jones Day *Alert*, EU Strikes Political Deal on Landmark Artificial Intelligence Act (Dec. 8, 2023).

87 *See* Jones Day *Commentary*, EU AI Act: First Rules Take Effect on Prohibited AI Systems and AI Literacy (Feb. 28, 2025).

88 *Supra*, note 87.

89 *See* Jones Day *Commentary*, European Commission's AI Code of Practice and Training Data Summary Template (Feb. 5, 2025).

90 *Supra*, note 84.

91 Jones Day *Commentary*, EU Enacts Broad Cybersecurity Requirements for Hardware and Software Products (Oct. 23, 2024); Jones Day *Alert*, European Commission Proposes Legislation Imposing New Cybersecurity Requirements on Digital Products (Sept. 27, 2022).

92 Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (Apr. 17, 2019) (Cybersecurity Act), recently amended by Regulation (EU) 2025/37 (targeted amendment to the Cybersecurity Act).

93 Regulation (EU) 2017/745 on medical devices (Apr. 5, 2017).

94 Regulation (EU) 2017/746 on in vitro diagnostic medical devices (Apr. 5, 2017).

95 Dep't for Sci., Innovation & Tech., A Pro-innovation Approach to AI Regulation (Aug. 3, 2023).

96 Dep't for Sci., Innovation & Tech., Copyright and Artificial Intelligence (Dec. 17, 2024).

97 Dep't for Sci., Innovation & Tech., AI Opportunities Action Plan (Jan. 13, 2025).

98 House of Lords, Artificial Intelligence (Regulation) Bill [HL] (Mar. 5, 2025).

99 Digit. Regul. Coop. F., DRCF to develop "one-stop" digital regulatory tool.

100 Digit. Regul. Coop. F., AI and Digital Hub.

101 Fin. Conduct Auth., AI Update.

102 Fin. Conduct Auth., AI Lab (Feb. 10, 2025).

103 Competition & Markets Auth., CMA AI Strategic Update (Apr. 29, 2024).

104 Dep't for Sci., Innovation & Tech., Assuring a Responsible Future for AI (Nov. 6, 2024).

105 *See* "Roadmap to trusted third-party AI assurance," UK Parliament (Sept. 3, 2025).

106 Dep't for Sci., Innovation & Tech., Government's Experimental AI Chatbot to Help People Set Up Small Businesses and Find Support (Nov. 5, 2024).

107 Dep't for Sci., Innovation & Tech., Ensuring Trust in AI to Unlock £6.5 Billion Over Next Decade (Nov. 6, 2024).

108 Copyright, Designs and Patents Act 1988, c. 48 § 29A (UK).

109 Fed. Trade Comm'n, FTC Announces Crackdown on Deceptive AI Claims and Schemes (Sept. 25, 2024).

110 *Fed. Trade Comm'n v. Rite Aid Headquarters Corp.*, No. 23-cv-05023 (E.D. Pa. Dec. 19, 2023).

111 Fed. Trade Comm'n, Aiming for Truth, Fairness, and Equity in Your Company's Use of AI (Apr. 19, 2021).

112 *Chamber of Com. v. CFPB*, case update (Apr. 30, 2025).

113 DOJ, "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," 28 CFR Part 202 (Jan. 8, 2025).

114 IRS, "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern," 31 CFR Part 850 (Nov. 15, 2024).

115 REAL Political Advertisements Act, H.R. 3044, 118th Cong. (2023–24).

116 NO FAKES Act of 2024, S. 4875, 118th Cong. (2023–24).

117 *See* NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices, NLRB, Office of Public Affairs, 202-273-1991 (Oct. 31, 2022).

118 Artificial Intelligence Research, Innovation, and Accountability Act of 2023, S. 3312, 118th Cong. (2023–24). *See also*, Algorithmic Accountability Act of 2023, H.R. 5628, 118th Cong. (2023–24); Artificial Intelligence Accountability Act, H.R. 3369, 118th Cong. (2023–24).

119 Federal Artificial Intelligence Risk Management Act of 2023, S. 3205, 118th Cong. (2023–24).

120 *See, e.g.*, S.B. 818, 2024 Gen. Assemb., Reg. Sess. (Md. 2024).

121 *See* Jones Day *Alert*, Colorado Enacts AI Consumer Protection Legislation (June 14, 2024).

122 *See* Jones Day *Alert*, Illinois Becomes Second State to Pass Broad Legislation on the Use of AI in Employment Decisions (Oct. 29, 2024).

123 Six states, including Colorado (H.B. 1147), New Hampshire (H.B. 1432), New Mexico (H.B. 182), Oregon (S.B. 1571), Utah (S.B. 131), and Wisconsin (A.B. 664), enacted legislation concerned with misinformation in political communications in the leadup to the 2024 election.

124 *See* Jones Day *Commentary*, California Enacts AI Transparency Law Requiring Disclosures for AI Content (Oct. 14, 2024).

125 A.B. 2013, 2023–2024 Gen. Assemb., Reg. Sess. (Cal. 2024).

126 Executive Order 14179, Removing Barriers to American Leadership in Artificial Intelligence (Jan. 23, 2025).

127 OMB M-25-21, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust (Apr. 3, 2025).

128 U.S. Department of Homeland Security, Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure (Nov. 14, 2024).

129 Executive Order 14141, Advancing U.S. Leadership in AI Infrastructure (Jan. 14, 2025).

130 Executive Order 14318, Accelerating Federal Permitting of Data Center Infrastructure (July 23, 2025).

131 *See* Jones Day *Alert*, White House Announces Artificial Intelligence Bill of Rights (Oct. 6, 2022).

132 FTC, "Children's Online Privacy Protection Rule," 16 CFR Part 312 (Apr. 22, 2025).

133 State Council, The State Council on Printing and Distributing Notice of the New Generation Artificial Intelligence Development Plan (July 20, 2017) (available in Chinese only).

134 Ministry of Sci. & Tech., Notice of the Ministry of Science and Technology on Printing and Distributing the 'Guidelines for the Construction of National New Generation Artificial Intelligence Open Innovation Platforms' (Aug. 8, 2019) (available in Chinese only).

135 Ministry of Sci. & Tech., Notice of the Ministry of Science and Technology on Printing and Distributing the 'Guidelines for the Construction of National New Generation Artificial Intelligence Innovation and Development Pilot Zones (Revised Edition) (available in Chinese only).

136 The State Forestry and Grassland Administration issued a Guiding Opinions on Promoting the Development of Artificial Intelligence in Forestry and Grassland in 2019.

137 The Ministry of Education, the National Development and Reform Commission, and the Ministry of Finance issued the Opinions on Promotion of Discipline Integration and Postgraduate Training in the Field of Artificial Intelligence in Colleges and Universities in 2020. These Opinions discuss courses and subjects development, international exchange of talents, cooperation with enterprises, and funding support, among others. The Ministry of Education also issued an Action Plan for AI Innovation in Colleges and Universities in 2018, aiming to enhance AI-related research, education, talents training, innovation, and application.

138 The State Food and Drug Administration issued the Guiding Principles for the Classification and Definition of Artificial Intelligence Medical Software Products, requiring registration and approval for AI-related medical software products and management of such products according to their medical instrument classification type.

139 The General Office of the Ministry of Housing and Urban–Rural Development approved Beijing and Shenzhen to experiment on using artificial intelligence to review construction drawings. Gen. Off. of the Ministry of Hous. & Urb.-Rural Dev., Letter from the General Office of the Ministry of Housing and Urban-Rural Development on the approval of Beijing (Sept. 16, 2020); Gen. Off. of the Ministry of Hous. & Urb.-Rural Dev., Letter from the General Office of the Ministry of Housing and Urban-Rural Development on the approval of Shenzhen (July 1, 2020).

140 Ministry of Sci. & Tech., Ethical Norms for the New Generation of Artificial Intelligence (Sept. 26, 2021) (available in Chinese only).

141 Nat'l Info. Sec. Standardization Tech. Comm., Notice on Issuing the "Guidelines for the Practice of Network Security Standards-Guidelines for Prevention of Artificial Intelligence Ethical Security Risks" (Jan. 1, 2021) (available in Chinese only).

142 Ministry of Econ., Trade & Indus., AI Governance in Japan Ver. 1.1: Report from the Expert Group on How AI Principles Should Be Implemented (July 9, 2021).

143 Version 1.0 of the AI Governance Guidelines was published for soliciting public comments on July 9, 2021. It was then finalized and published as Version 1.1 on Jan. 28, 2022.

144 Conference Toward AI Network Society, Draft AI R&D Guidelines for International Discussions (July 28, 2017).

145 Conference Toward AI Network Society, AI Utilization Guidelines Practical Reference For AI Utilization (Aug. 9, 2019).

146 Report 2022: Further Promotion of "Social Implementation of Safe, Secure and Reliable AI" (available in Japanese only).

147 Ministry of Internal Affs. & Commc'ns, AI Guidelines for Business Ver 1.0 (Apr. 19, 2024).

148 Directive (EU) 2024/2853 on liability for defective products (Oct. 23, 2024).

149 Council Directive 85/374/EEC on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (July 25, 1985). The European Union had also been considering an AI Liability Directive, but it has been abandoned as of publication. *See* European Parliamentary Research Service, Proposal for a Directive on Adapting Non-contractual Civil Liability Rules to Artificial Intelligence: Complementary Impact Assessment (Sept. 19, 2024).

150 *See*, in particular, the Staff Working Document on Liability accompanying the EU AI Strategy (SWD (2018)137).

151 For example, in a 2019 report, the Commission's Expert Group on Liability and New Technologies examined liability issues in connection with AI technologies. The Expert Group concluded that contractual or tort liability systems do exist in the Member States, but these insufficiently cover all circumstances that justify liability. Consequently, it remains necessary to close these liability gaps.

152 On June 30, 2021, the Commission also issued an inception impact assessment. On Oct. 20, 2020, the European Parliament adopted a resolution, which included a draft for a Regulation on liability for the operation of artificial intelligence systems.

153 Eur. Comm'n, Commission Consultation, Civil Liability—Adapting Liability Rules to the Digital Age and Artificial Intelligence.

154 *See* Jones Day *Alert*, Radical Changes to Europe's Product Liability Rules Adopted (Nov. 27, 2024).

155 Competition & Mkts. Auth., Consumer Protection: Enforcement Guidelines (Jan. 23, 2025).

156 *See, e.g.*, S.B. 213, 75th Gen. Assemb., 1st Reg. Sess. (Colo. 2017) (stating that liability for a crash involving an autonomous vehicle not under human control is determined in accordance with applicable state law); H.B. 311, 2019 Leg., Reg. Sess. (Fla. 2019) (establishing that an "automated driving system, when engaged, shall be deemed to be the operator" of a vehicle, creating potential liability for the manufacturer).

157 Utah Code Ann. § 76-2-107 (West 2024).

158 *See* Jones Day *Alert*, SEC Chair Warns Against "AI Washing" (Dec. 12, 2023).

159 *See* Jones Day *Commentary*, SEC's and Private Litigants' Continued Focus on "AI Washing" (Oct. 23, 2024).

160 *See* Jones Day *Commentary*, Court Grants Summary Judgment in AI Copyright Clash, Rejecting "Fair Use" (Feb. 25, 2025).

161 43 F.4th 1207 (Fed. Cir. 2022).

162 *See* Jones Day *Commentary*, USPTO Issues New Guidance for Inventions Assisted by Artificial Intelligence: Human Contribution is Key (Feb. 15, 2024).

163 *Thaler v. Perlmutter*, No. 23-5233 (Fed. Ct. of App. DC Cir. Mar. 18, 2025).

164 *See* Jones Day *Commentary*, Copyrightability of AI Outputs: U.S. Copyright Office Analyzes Human Authorship Requirement (Feb. 20, 2025).

165 *See* Jones Day *Commentary*, AI and Deepfakes: U.S. Copyright Office Urges Federal Digital Replica Law (Aug. 15, 2024).

166 Jones Day *Commentary*, U.S. Copyright Office Issues Guidance on Generative AI Training (May 22, 2025).

167 China News, Nine Model Civil Cases of Judicial Protection of Personality Rights after the Issuance of the Civil Code Published by the Supreme People's Court (Apr. 11, 2022) (available in Chinese only).

168 Ten Typical Cases on Serving and Protecting New Quality Productive Forces (Aug. 26, 2024) (available in Chinese only). One of these cases ruled that the individual plaintiff's rights to his voice were personal rights, which extended to AI-synthesized voice and had been infringed by the defendants. The court found that the voice synthesized using AI by the defendants can be specifically associated with the plaintiff by the general public or professionals in the relevant field based on its tone, intonation, and pronunciation style, and therefore it can be considered identifiable.

169 Civil Code, Act No. 89, pts I–III (1896).

170 Product Liability Act, Act No. 85 (1994).

171 The term "defect" is defined as a "lack of safety that a product should normally have, taking into account the characteristics of the product, the normally foreseeable usage manner, the time at which the manufacturers, etc. delivered the product, and other circumstances of the product." Product Liability Act, art. 2, para. 2 (1994).

172 *See* Jones Day *Alert*, The Tokyo District Court Holds an Artificial Intelligence Systems Cannot Be an Inventor Under Japanese Patent Law (June 20, 2024). The Intellectual Property High Court upheld the Tokyo District Court's decision on Jan. 30, 2025.

173 Dep't of Indus., Sci. & Resources, The Legal Landscape for AI in Australia.

174 *Australian Competition and Consumer Commission v Trivago N.V.* [2020] FCA 16.

175 China's Prohibited and Restricted Export Technology Catalogue (2023) (available in Chinese only).