JONES DAY | One Firm Worldwide®

# WHITE PAPER

December 2022

## Rising Global Regulation for Artificial Intelligence

Across multiple continents and industries, artificial intelligence ("AI") is a topic of intense focus by governments, research institutions, investors, and corporations—from start-ups to well-established industry players. As technology and regulatory frameworks continue to evolve rapidly, AI legal issues are emerging as a key topic in a transactional, litigation, and regulatory compliance context.

This *White Paper* outlines key AI regulatory issues and questions that are worthy of consideration by private-sector leaders and in-house counsel.

## TABLE OF CONTENTS

## INTRODUCTION

Across a wide range of industries, including advertising, banking, telecommunications, manufacturing, transportation, life sciences, waste management, defense, and agriculture, the use of AI and interest in its diverse applications are steadily increasing. 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 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.

Yet the recent surge of interest in AI sometimes obscures the fact that it remains ungoverned by any 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 may implicate areas of law that developed largely before AI became prevalent. Because it is an intangible process that 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 or litigate AI-related issues.

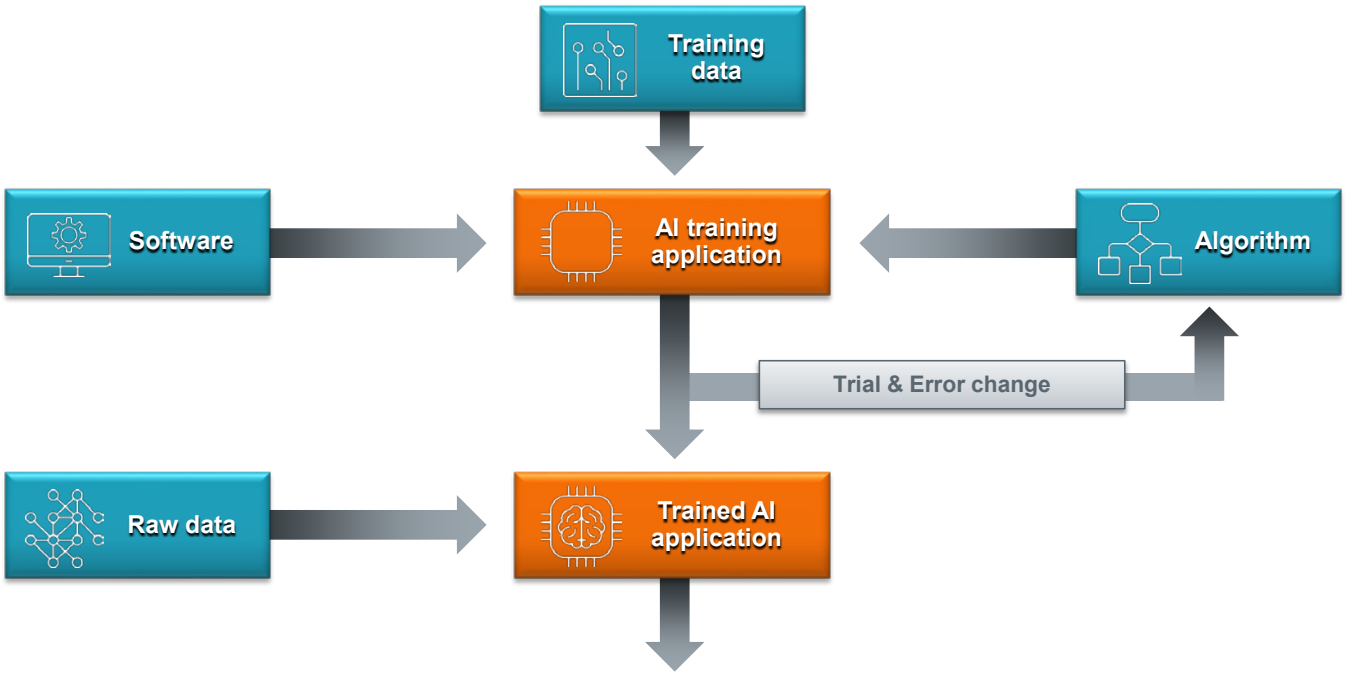
This *White Paper* seeks to demystify AI for nontechnical readers, and reviews the core legal concepts that governments in several key jurisdictions—the European Union, China, Japan, and the United States —are developing in their efforts to regulate AI and encourage its responsible development and use. Although AI legal issues facing companies will often be specific to particular products, transactions, and jurisdictions, this *White Paper* also includes a checklist of key questions that in-house counsel may wish to address when advising on 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. This scenario, which calls for patient review and a strategic perspective by regulated parties, rewards an ability to explain technical products to regulators in clear, nontechnical terms.

## 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 allowing such models to be used in processing and making autonomous decisions, for example.

Key to each AI is its "objective function"—the goal or goals that its developers have designed it to achieve. This objective function can vary widely—from identifying molecules with likely antibiotic properties, to predicting where and when inputs in a transportation or manufacturing system will be needed, to spotting potential safety or security threats, to generating text, sound, or images that meet certain specifications. To learn to achieve this objective function, AI models can be trained using large data sets—with varying degrees of human oversight and feedback—learning to identify and make predictions based on patterns, likenesses, and fundamental attributes, including ones that humans may never have conceptualized or perceived. The AI is then prompted to apply the model it has honed during training to a real-life situation, where it executes its task. This latter activity is often referred to as "inference."

## ARTIFICIAL INTELLIGENCE (AI) COMPONENTS




AI components typically comprise data (both training data for training and raw data for inference) and software processes to execute complex algorithms.

When trained and applied correctly, AI-based technology can unlock tremendous gains in productivity—enabling results or insights that would otherwise require prohibitively long periods of time to achieve by means of human reason alone, or even by humans using traditional computing techniques. In some cases, AI can be applied to replace or augment "rote" tasks that a person would otherwise perform much more slowly. In other cases, AI can generate text (including computer code, or responses to basic customer queries), sound, or images (including aspects of architectural or mechanical designs) that either replace the need for human input or serve as a first draft for human review. Often, a human mind, informed by AI inputs, analysis, and recommendations, can home in faster on a key range of options (pharmaceutical, strategic, etc.) warranting closer study.

In many industries, integrating AI-based technology is considered the key to secure 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. In addition, governments seek to support AI's growth through a legislative framework that allows the technology to develop and optimize its potential.

However, as many governments and analysts have noted, the benefits of AI systems can also come with risks. For example, AI can contribute to the creation of "echo chambers" that display content based only on a user's previous online behavior and thereby reinforce their views and interests or exploit their vulnerabilities. AI applications are also increasingly used in objects routinely interacting with people, and could even be integrated in the human body, which can pose safety and security risks.

Governments seeking to regulate AI aim to build citizen trust in such technology while limiting potentially harmful applications. Yet different governments, and different agencies within the same government, sometimes have different concepts of what constitutes an appropriate manner of training and applying 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 key considerations

such as privacy, transparency, liberty, and security. As governments apply divergent perspectives to this technically complex (and often inherently multijurisdictional) area, regulated parties face a complex, sometimes contradictory body of regulatory considerations that are themselves 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?

While many laws already apply to AI, ranging from IP protection to competition law and privacy, AI's rapid expansion has alerted legislators worldwide, leading to updating legal and regulatory frameworks and, in some cases, creating entirely new ones. These global legal initiatives generally aim at addressing three main categories of issues:

- First, legislation and regulations aim to foster AI deployment by creating a vibrant and secure data ecosystem. 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 hunger for data is regulated in part through the well-known GDPR; additionally, a proposed Data Act facilitating data access and sharing is underway. In comparison, the United States has taken a more decentralized approach to the development and regulation of AI-based technologies and the personal 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 in the course of Congressional hearings or agency investigations rather than through clearly proscriptive published rules. The People's Republic of China, for its part, has expanded its data security and protection laws, with a particular emphasis on preventing unauthorized export of data. 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.
- Second, regulators in multiple jurisdictions have proposed or enacted restrictions on certain AI systems or uses assessed to pose safety and human rights concerns. Targets for such restrictions include AI robots 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 socio-economic discrimination. In the European Union, the sale or use of AI applications may become subject to uniform conditions (e.g., standardization or market authorization procedures). For instance, the proposed EU AI Act aims to prohibit market access for high-risk AI systems, such as AI systems intended for the "real-time" and "post" remote biometric identification of natural persons. 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. The PRC and Japan have not yet issued mandatory laws or regulations restricting application of AI in any specific area for concerns such as discrimination or privacy. But similar to the United States, China regulates various aspects important to the realization and development of AI, such as data security, personal information protection, and automation, among others.
- 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, in order to facilitate consumer damage claims. The first comprehensive proposal comes from the European Union's new draft liability rules for AI systems, aimed at facilitating access to redress for asserted "victims of AI," through easier access to evidence, presumption of causality, and reversal of the burden of proof.

Each of these will be further discussed in the next 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 data sets. To achieve a thriving data ecosystem that meets such 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 data sets 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 data sets 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 concerns.

### European Union

**Current Legislation.** 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 General Data Protection Regulation ("GDPR").[1] By seeking to establish a human-centric approach to technology and to ensure that individuals can better control that their personal data is processed only for a legitimate purpose in a lawful, fair, and transparent way, the GDPR aims to establish a solid framework for digital trust, while providing for free movement of personal data within the European Union and regulating international data flowing outside the European Union. 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.[2] 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.

For non-personal data, the European Union adopted a Regulation on the Free Flow of Non-Personal Data[3] in 2018 to ensure free movement of such data and prohibit Member States from adopting (restrictive) data localization laws similar to other jurisdictions such as Russia. Additionally, the European Union's Open Data Directive[4] 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").

**Upcoming Legislation.** In 2020, the European Union announced a European Strategy for Data[5] 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 both 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")[6] in June 2022, which aims at facilitating voluntary data sharing by individuals and businesses through enhanced trust in such sharing. The DGA promotes trusted sharing through neutral data brokers notified to the public authorities 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 Commission also proposed a Data Act[7] in February 2022. This proposed Regulation seeks to facilitate voluntary business-to-business data sharing and to further business-to-government data sharing in case of urgency. The proposed Data Act also reviews the existing intellectual property rights framework in order to facilitate data access and use.

In parallel, the European Union is also developing sector-specific data regulation to boost the EU data economy. EU law already provides for some forms of data sharing obligations in the banking sector for payment data,[8] in the energy sector for smart meter/consumption data,[9] and data provided to or created by digital content/services (all concerning personal data);[10] as well as in the automotive sector for repair and maintenance information[11] and intelligent transport systems[12] (including potentially in-vehicle data[13] and alternative fuels infrastructure[14]) (all non-personal data). The Digital Market Act ("DMA"),[15] 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 available data generated by business users 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 nine areas.

| EU Data Spaces | | |
|---|---|---|
| Industrial (manufacturing) | Green Deal | Mobility |
| Skills | Health | Financial |
| Energy | Agricultural | Public Administrations |

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.[16] The draft 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 | Status |
|---|---|---|---|
| **General** | | | |
| **GDPR** | 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 | In force since July 16, 2019; Member State implementation by July 17, 2021 |
| **DGA** | All data | G2B data sharing | Entry into force on June 23, 2022, and applicable from September 2023 |
| **Draft Data Act** | All data | B2B sharing<br>B2G data sharing | Proposal submitted on February 23, 2022 |
| **Sector-Specific** | | | |
| **DMA** | Certain data held by "gatekeepers" | B2B sharing | Entry into force on November 1, 2022, and applicable from May 2, 2023 |
| **PSD2** | Payment data | Open payment services | Applicable since January 13, 2018 |
| **Electricity Directive** | Smart meter/consumption data | Energy consumption data availability | In force since July 4, 2019; Member State implementation by December 31, 2020 |
| **Gas Directive** | Smart meter/consumption data | Energy consumption data availability | In force since July 13, 2009; Member State implementation by March 3, 2011 |
| **Digital Content and Services Directive** | Digital content/services data | Digital content/services | In force since June 11, 2019; Member State implementation by July 1, 2021 |
| **Motor Vehicle Regulation** | Repair and maintenance data | Aftermarkets for repair | Applicable since September 1, 2020 |
| **Draft ITS Directive** | Intelligent transport systems data | Smart transport systems | Proposal submitted on December 14, 2021 |
| **Draft Recharging Infrastructure Regulation** | Recharging infrastructure data | Interoperability of recharging infrastructure | Proposal submitted on July 14, 2021 |
| **Draft In-Vehicle Data Regulation** | In-vehicle data | Autonomous vehicles | Proposal expected in 2023 |
| **Draft European Health Data Space Regulation** | Health data | B2B sharing in health sector | Proposal submitted on May 3, 2022 |

**Regulatory Oversight of Data Ownership, Data Pooling, Data Access, and Portability.** Data increases in value when available in large pools. This need for big data 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 though 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 would be limited to only certain circumstances,[17] also when done through trade associations.[18] Similarly, competition authorities could investigate practices whereby certain dominant companies refuse to provide data akin to an essential facility.[19]

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 included rules on the porting of data for professional users via industry codes of conduct. The DMA also includes rules allowing the portability of data held by gatekeepers and sets out data access rights for business users of gateway service providers (such as online marketplaces).

The proposed Data Act now seeks to bring access and data portability to an entirely new level, as it would include general access and portability rights applicable to all data holders, in particular in the cloud sector. The proposed Data Act would also limit 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.[20] 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.

**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.

Work on a substantive legal framework to regulate AI's development and use has been comparatively slow, with a handful of federal agencies addressing 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 ("FDA") proposed a regulatory framework for AI-based software incorporated into medical devices.
- 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 more searching review.
- The Department of Commerce's NIST (National Institute of Standards and Technology), the Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau ("CFPB"), and the Federal Housing Finance Agency ("FHFA") have each promulgated guidelines aimed at protecting consumers from misuse of AI.

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. As might be expected, 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.

**Limited Data Access Through Voluntary Standardization.** Data access is critical to promoting and maintaining a vibrant AI ecosystem. Likewise, standardization efforts can sometimes act to 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 the NIST, created in 1901 and housed within the Department of Commerce. NIST's mission regarding AI is to research and develop standards for AI 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, the 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 both the government and private industry. 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, the NIST is preparing an AI risk management framework ("AI RMF"), a guidance document to help manage AI's potential risks to individuals, organizations and society. The NIST released a first draft of the AI RMF in March 2022 and a second draft in August 2022, each time requesting comments. The draft AI RMF establishes 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.

Legislative efforts at promoting 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 aimed at encouraging 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. Pending legislation in Hawaii would establish an income tax credit for investment in qualified businesses that develop cybersecurity and AI within the state.

**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 every online interaction has long worried privacy advocates. In the United States, nationwide regulation for data protection exists only for specific segments of the population. For example, the Health Insurance Portability and Accountability Act ("HIPAA") governs how personal health information can be accessed and shared, while the Family Educational Rights and Privacy Act, or 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 that AI-based technologies rely on.

In the absence of federal legislation, individual states are starting to pass laws aimed at enabling 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 requires businesses to disclose the consumer's right to delete 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. Both acts mirror the CCPA and seek to give consumers more control over data collection. Similar proposed bills on data privacy are currently pending in New York, while one recently failed in the state of Washington.

In short, recent federal efforts in the United States have largely focused on promoting AI policy and standardization, leaving states to regulate data privacy. With regard to data accessibility for individuals, consumers and privacy advocates have called 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 (FTC) 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 |
| **California Consumer Privacy Act (CCPA)** | Personal data | Provides privacy protection for California consumers | January 1, 2020, with amendments by the California Privacy Rights Act that go into effect on January 1, 2023 |
| **Data specific** | | | |
| **Health Insurance Portability and Accountability Act (HIPAA)** | Certain medical information | Protects protected health information held by covered entities | August 21, 1996 |

*continued on next page*

| Name of Legislation | Type of Data | Main Purpose | Effective Date |
|---|---|---|---|
| **Fair Credit Reporting Act (FCRA)** | 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 (FERPA)** | Student education records | Governs access to educational information and records by public entities | August 21, 1974 |
| **Data specific** | | | |
| **Gramm-Leach-Bliley Act (GLBA)** | 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 (COPPA)** | Data from minors | Imposes certain limits on data collection for children under 13 years old | April 21, 2000 |

**China**

The PRC does not restrict AI's use or development in an AI-specific legislation. However, the PRC is regulating elements needed to build AI technologies, including data (e.g., personal information, facial recognition, big data, algorithm, or automated decision-making).

**Data Protection.** The PRC boosted its regulation of data protection in 2021 by enacting the PRC Personal Information Protection Law ("PIPL").[21] Notably, consent is required to obtain an individual's personal information, unless one of a limited number of exceptions applies.[22] 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.[23] The PRC Antitrust Law (2007) further provides that business operators may not use data, algorithms, technology, etc., to engage in monopolization.[24]

The PRC also recently tightened data security through its Measures for the Security Assessment of Outbound Data Transfer (2022).[25] Under these Measures, the international exchange of AI knowledge or information may be problematic, since data involved in the development or application of AI might be deemed important data. Thus, any international transfer of such data would trigger the data handler's obligation to apply for a security assessment to seek the review and pre-approval of the PRC government. High-end chips, devices, or other technologies may also be the subject of national security and thereby considered highly confidential and prohibited from sharing.

PRC regulators remain well-aware that the promotion of free flow of data is crucial to the larger-scale application of AI. The PRC encourages the free flow of data and information within the framework of the above-mentioned protective laws and regulations. For example, local governments are exploring methods to facilitate data sharing or trading, such as by establishing platforms for collection and access to big data, setting up data exchange centers, or designating a new "free trade" zone for the free flow of data, and particularly for international data transfers.[26]

**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").[27] Under the APPI, consent is not required to collect personal information, except 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.[28] For transfer of personal data to a third party, the APPI in principle requires data subjects' advance consent unless any exception applies.[29] Additionally, in principle, cross-border transfer of personal data requires consent unless any exception applies.[30] The APPI's recent 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.[31]

**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 so that a person cannot be identified in accordance with the strict processing rules set forth in the APPI implementation regulations and related guidelines, this anonymously processed information[32] can be transferred to a third party without data subjects' consent, but is subject to additional strict obligations and requirements imposed on the parties creating and using such information.
- **Anonymized medical information.** Medical data is very useful big data 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 use of such medical data than other types of personal data. Collection of sensitive personal information, such as medical history, requires advance consent of the data subjects.[33] 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.[34]

  In order to facilitate use of personal medical data for medical research and development purposes, Japan established secure rules to create and use anonymized medical information, enacting the Act on Anonymized Medical Data to Contribute the Research and Development in the Medical Field (Act No. 28 of May 12, 2017) ("Next Generation Medical Infrastructure Act"),[35] which took effect with the relevant cabinet ordinances and guidelines on May 11, 2018. Under this Act, medical institutions can collect and provide medical information to organizations certified to anonymize medical information without obtaining consent from patients, who only need to be notified of certain required items, including the patient's right to opt out.[36] The certified organization then anonymizes the medical information and can provide it to other organizations for use in medical research and development.
- **Voluntary sharing of personal data—certified information banks.** Businesses can be certified as information banks to promote and facilitate the voluntary exchange and sharing of personal data under the APPI's consent requirement regime. Individuals can entrust the handling of certain personal information (including use of smartphone applications, browsing history, purchase records, location data, etc.) to an information bank, providing consent for the information bank to disclose this information to other business entities subject to certain terms and conditions. In return for consenting to disclose this personal data, individuals receive benefits such as discount coupons from the receiving business entities. To establish standards and rules for certification of information banks, the Ministry of Internal Affairs and Communications ("MIC") and the Ministry of Economy, Trade, and Industry ("METI") together prepared and published "Guidelines Regarding Certification of Information Entrustment Function" in June 2018 (ver. 1.0).[37] Certification as an information bank is voluntary and not required for engaging in this activity, but it is useful to show the organization's credibility and its compliance with security measures to protect privacy.

**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.[38] The report confirmed that the current Anti-Monopoly Act (Act No. 54 of April 14, 1947, as amended)[39] may apply to and regulate unfair data pooling and lock-in by monopoly and oligopoly firms (e.g., "unreasonable restraint of trade," "unfair trade practices").

## 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. In just a few examples:

- Algorithms that have the purpose or effect of serving to set up a price cartel 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 in the United States and the European Union.
- The use of AI systems in selecting job applicants or determining the creditworthiness of borrowers may raise issues related to statutory anti-discrimination protections. Allegations may focus on various factors. For instance, an algorithm may be trained with a historic data set that is identified as reflecting bias, allegedly amplifying past discriminatory hiring practices. Similar effects might also arise from the underrepresentation of a group in the data set or the selection of analyzed characteristics.

**The Case of Clearview AI**

Clearview AI offers services (with a reported focus on law-enforcement customers) that allow facial recognition based on an extensive database of pictures "scraped" from the internet (social media, etc.).

In the European Union, several data protection authorities adopted decisions prohibiting the use of Clearview AI technology, based on the lack of legal basis to process biometric data (pictures).

In the United States, Clearview AI agreed to cease selling individual access to its database inside the country and committed to destroy its existing stock of facial-recognition vectors under the terms of a settlement reached with the American Civil Liberties Union.

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**

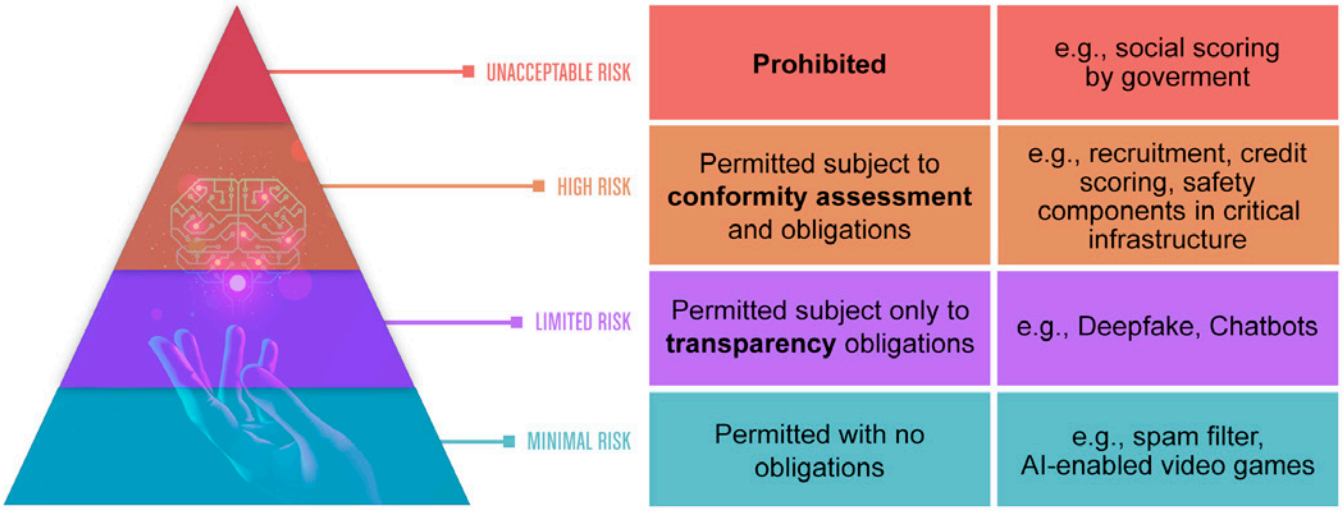
**Current Legislation.** An extensive body of existing EU product safety legislation potentially applies to various AI applications, but attempting to apply this existing legislative framework to new AI systems has raised various problems. For instance, the European Union's current general product safety legislation (dating from 2001) has a limited scope that applies only to products, thereby excluding AI-based services, such as those related to health, financial, or transport services.

In setting out an AI strategy,[40] the European Union sought to promote the uptake of AI while addressing the associated risks. One important aspect is regulating market access in view of ensuring user safety and safeguarding fundamental EU values and rights. After recognizing loopholes in current 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[41] outlining necessary policy changes and investment at Member State level, the Commission also set out two proposed Regulations aimed at harmonizing safety requirements and market access of AI applications at the EU level: (i) the AI Act and (ii) the General Product Safety Regulation (to replace the current General Product Safety Directive).

**Proposed AI Act.** The Commission's proposed AI Act,[42] published in April 2021, aims at harmonizing rules for bringing to market, putting into service, and using AI systems in the European Union (*see also,* "Regulating Artificial Intelligence: European Commission Launches Proposals," Jones Day *Commentary*, Apr. 2021).

Under the proposal's risk-based approach (see figure below):

- Certain AI practices are prohibited, as they are considered as 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; and
- Certain low-risk AI systems, like deepfakes, are subject to harmonized transparency rules.




On enforcement, market monitoring and surveillance is ensured by national regulators with the ability to impose significant fines, under the supervision of an anticipated European Artificial Intelligence Board.

The proposed AI Act is currently expected to be adopted by year-end 2022, enter into force in 2023, and become applicable two years after its entry into force.

**Preventing Biases.** The proposed AI Act 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 design.

While the GDPR can already catch some biases (e.g., though its data accuracy obligation and prohibition of decision-making based solely on profiling), the proposed AI Act may further limit bias risks. Its high-risk AI requirements minimize the risk of algorithmic discrimination, particularly in relation to the quality of data sets used for developing AI systems and the obligations for testing, risk management, documentation, and human oversight throughout the entire AI system's lifecycle.

**Proposed General Product Safety Regulation.** Toward adapting current legislation to new technologies and its related challenges, the Commission also proposed a Regulation on General Product Safety in June 2021.[43] This would replace the General Product Safety Directive,[44] whose statutory safety requirements must be met before bringing products to market. The proposed Regulation aims to broaden the current Directive's scope to cover, in particular, AI systems. For example, as mentioned above, the existing General Product Safety Directive's limited scope applies only to products and does

not cover AI-based services. The proposed Regulation would expand definitions, such as "product" and "safety," to enable regulating new technologies. Furthermore, current EU product safety legislation focuses on a producer placing its product on the market. This means that such legislation does not cover stand-alone software (which is not the final product) or third parties that introduce an AI component to a product after its introduction on the market. These cases will now be covered in the new proposal.

**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 to the extent that these rules would facilitate cross-border trade by businesses. These include the EU Cybersecurity Act,[45] 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,[46] in force since 2017, whose rules include software medical devices; the Regulation on In-Vitro Diagnostic Medical Devices,[47] in force since 2017; and the Commission proposal for a Cyber Resilience Act submitted on September 15, 2022[48] (*See also*, "European Commission Proposes Legislation Imposing New Cybersecurity Requirements on Digital Products," Jones Day *Alert*, Sep. 2022).

**United States**

**Patchwork of Competent Authorities.** Federal enforcement authorities have expressed concerns for the potential misuse of AI-based technologies, especially as such misuse might affect individuals. Congress has not enacted 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.

The FTC was one of the first agencies to assert a role in preventing the misuse of AI-based technologies, via a blog post in April 2021. While helpful to illustrate the agency's priorities, this guidance does not bind regulated parties. The FTC claims to draw its asserted authority to curb potentially 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. These theories remain controversial and are subject to ongoing challenges in the courts. The FTC blog post encourages companies to start with solid AI foundations and improve their data sets, to be mindful of the potential for discriminatory outcomes, and to embrace transparency. Further, the post urges companies to disclose data collection when engaging with consumers. The post cites an FTC complaint alleging that a social media company misled users about their ability to opt out of their facial recognition software as evidence of the FTC's willingness to go after companies that engage in "data malpractice." The FTC goes on to note that even inadvertent violations will be pursued, and that if a company's AI algorithm results in, for example, credit discrimination against a protected class, the FTC can file a complaint. Finally the post ends with a warning for companies to "hold yourself accountable—or be ready for the FTC to do it for you."

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

- The Equal Employment and Opportunity Commission announced the launch of an 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") announced a proposed rulemaking by which algorithms used in housing decisions potentially could be challenged as having a discriminatory impact or effect. This rule, if finalized, is expected to be challenged on the grounds that it exceeds HUD's authority under the Fair Housing Act, as interpreted by the U.S. Supreme Court.
- The CFPB controversially asserted in March 2022 that its "unfairness" authority may be used to regulate anti-discrimination. 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." Industry trade associations recently brought litigation challenging this as exceeding the CFPB's authority as prescribed by Congress under the Dodd-Frank Act and the Equal Credit Opportunity Act. They argue that Congress did not intend for the CFPB to regulate discrimination.

- Finally, the FHFA released an advisory bulletin in February 2022 that provides AI and machine-learning risk management guidance for Fannie Mae and Freddie Mack, and it is the first publicly released guidance by a U.S. financial regulator that is focused on AI risk management.
- Agencies whose primary concerns with AI are not focused on these potentials for discrimination have weighed in on the role these technologies are likely to play in their fields. For example, the FDA is proceeding forward with its 2019 Action Plan on Artificial Intelligence/Machine Learning-Based Software as a Medical Device. The Plan proposes changes to the traditional paradigm of medical device regulations for devices that incorporate or predominantly rely on AI and machine learning. The new approach would provide for a premarket program for such devices. However, the FDA states this would require a commitment from manufacturers on transparency and real-world performance monitoring as a part of the premarket submission process.

**AI Prohibitions.** The U.S. legislative approach to AI prohibition is likewise piecemeal and predominantly issue driven. One prominent example is the 2020 Identifying Outputs of Generative Adversarial Networks, or IOGAN, Act. The Act directs the National Science Foundation and the NIST to support research on "deepfakes" (also referred to as "machine-manipulated media" or "digital content forgeries"), which are highly realistic AI-created media. The Act aims to encourage technology to detect deepfakes for both consumer protection and national security purposes—implicitly recognizing that a statutory prohibition on specific types of content or content generation could raise significant constitutional questions.

**AI Bill of Rights.** On October 4, 2022, the White House Office of Science and Technology Policy published the blueprint for an AI Bill of Rights, 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. (*See*, "White House announces Artificial Intelligence Bill of Rights," Jones Day *Alert*, Oct. 2022.)

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. To achieve and guarantee this, automated systems should undergo regular monitoring designed 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. Discriminatory uses of algorithms and algorithms that generate discriminatory results should be abolished and prohibited.
- Data privacy. Users sharing their data should have agency over how their data is used and be protected from abusive data practices. As such, companies should include built-in data protections and 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.

While the AI Bill of Rights sets forth voluntary guidelines only, it may set the stage for future legislation and regulations surrounding the use and implementation of AI.

### China

**Promoting AI.** China's State Council issued a "Development Plan on the New Generation of Artificial Intelligence" ("Plan") in 2017.[49] The 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 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.

With this context in mind, the Development Plan sets out the country's main tasks, including, among others, promulgating laws, regulations, policies, and ethical rules that promote or regulate AI development, and establishing an AI security monitoring and evaluation system to manage any abuse of data, infringement of personal rights, network security, or other potential issues.

In 2019, for the purpose of implementing the Development Plan, the Ministry of Science and Technology issued "Work Guidelines for the Construction of National Open Innovation Platforms for New Generation Artificial Intelligence."[50] The Work Guidelines identify enterprises as the main actors or leaders for constructing AI-related open-source platforms, sharing technology and research resources with the public, and relying on the market to provide funds and continuous support for such platforms. The Work Guidelines encourage cooperation among local governments, industries, research facilities, and universities and the integration of resources for the purpose of developing such platforms. The Work Guidelines list the requirements and procedures applicable to businesses leading the construction of such AI-related platforms in specific industrial areas.

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" in 2020.[51] 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 multiple cities for the development of such pilot zones, such as Harbin, Shenyang, and Zhengzhou.[52]

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,[53] higher education,[54] medical software products,[55] and construction.[56]

**Guidance.** Several government agencies (e.g., the National Standardization Administration, the Central Cyberspace Administration Office, the National Development and Reform Commission, the Ministry of Science and Technology, and others) issued "Guidelines for the Construction of the National New Generation Artificial Intelligence Standard System" in 2020. The Guidelines set out eight main categories of various AI-related subjects for which standards are to be promulgated:

- Basic and common standards (e.g., terminology or knowledge structure, testing, or evaluation);
- Supporting technology or products (e.g., algorithms, big data, data storage);
- Basic AI software or hardware platforms (e.g., chips, systematic software, development framework);
- Key general technologies (e.g., machine learning, calculation, identification);
- Technologies in key areas (language or vision processing, biometrics, virtual reality, human-machine interaction);
- Standards for AI products or services, including industrial standards (e.g., AI's application in manufacturing, agricultural, transportation, medical treatment, education, and public governance);
- Safety standards; and
- Ethical standards.

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").[57] This 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.

**Japan**

Japan has chosen to provide only non-legally binding guidelines, with the intention of leaving AI's use and development undeterred. This contrasts the EU-style horizontal and comprehensive regulatory approach to AI, as well as U.S.-style specific and targeted regulations.

On July 9, 2021, METI published a report titled "AI Governance in Japan ver. 1.1" ("AI Governance Report").[58] 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").[59] The AI Governance Guidelines consist of: (i) action targets to be implemented; (ii) practical examples that correspond to each action target; and (iii) practical examples for the purposes of carrying out gap analysis between AI governance goals and current circumstances. The AI Governance Guidelines present in total 21 action targets in accordance with the six categories of: (i) conditions and risks analysis; (ii) goal setting; (iii) system design; (iv) implementation; (v) evaluation; and (vi) re-analysis of conditions and risks. The action targets are general and objective targets that should be implemented by every AI company involved in the AI business—typically, the development/operation of AI systems that could have a certain level of negative impact on society.[60] On the other hand, the practical and gap analysis examples cannot take into account the individual and specific circumstances of every AI company. Accordingly, as the Guidelines indicate, each AI company will determine whether and how to adopt the practical and gap analysis examples to achieve the action targets in light of its own situation.[61]

Separately, MIC, through the Conference toward AI Network Society, published "Draft AI R&D Guidelines for International Discussions"[62] on July 28, 2017, and "AI Utilization Guidelines Practical Reference for AI Utilization"[63] on August 9, 2019. According to its 2022 Annual Report,[64] the Conference is considering the review and amendment of these guidelines in light of recent developments in these areas.

## 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), etc.

**European Union**

**Current Legislation.** Member States essentially oversee liability regimes, with only a small part harmonized at EU level. In particular, the Product Liability Directive imposes strict liability on producers for their defective products,[65] but it regulates only certain types of damages and applies only in the event of a defect in a product.

**Specific Liability Rules for AI.** The EU AI strategy (and its annexes[66]), as well as related expert reports[67] and communications,[68] concluded that further harmonization of liability rules was required to address AI's specificities. Following a consultation in October 2021,[69] the European Commission published two new proposals on September 28, 2022:

First, the proposed Revised Product Liability Directive aims at modernizing the current EU framework on manufacturers' liability for defective products to include the following points:

- Extending the definition of "product" to enable strict liability rules to cover intangible products such as software and AI. At present, since most software and applications can be classified as a "service" rather than a "product," these do not fall under the scope of the current Product Liability Directive.
- Broadening the scope of damages to include cyber vulnerabilities (e.g., connectivity and cybersecurity) and nonmaterial damage (e.g., loss of data, environmental damage).
- Widening the strict liability regime for importers to include 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 would be subject to strict liability rules.
- Extending the notion of "defect" to cover defective refurbished or remanufactured products and defective spare parts that cause damage. This expansion would address the fact that AI systems continuously learn and develop while operating, and are continuously updated with new data and software. Reliance on the so-called "development risk defense" (essentially a state-of-the-art standard at the time of conception) would also be denied for AI products that continue to learn and adapt while in operation.
- Facilitating claims to compensation by requiring manufacturers to disclose necessary information in court and by easing the burden of proof for victims in more complex cases, as in those involving AI-enabled products.

Second, the proposed AI Liability Directive provides for a targeted harmonization of national civil liability rules for AI. It supplements the rules under the above-described proposed Revised Product Liability Directive by introducing two main additional measures specifically for AI in noncontractual civil law claims for damages:

- Alleviating victims' burden of proof through the "presumption of causality," whereby courts can establish the causal link between the damage and noncompliance of providers of AI systems with a certain obligation relevant to the harm (e.g., with a duty of care under EU or national law), if the victims can demonstrate such noncompliance. This presumption is rebuttable by proving that a different cause provoked the damage.
- Empowering courts to order providers of high-risk AI systems (as defined under the proposed AI Act) to disclose relevant information, subject to appropriate safeguards to preserve the legitimate interests of all parties, such as trade secrets or other sensitive information.

The proposal for a revised Product Liability Directive would harmonize liability rules across EU countries and thus reduce legal fragmentation. However, such harmonization would be limited to tort law, while national laws would continue to govern contractual liability (including liability exemptions, etc.).

**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 updating their general tort laws to cover certain AI-based damages. For example, many states have passed legislation related to autonomous vehicles to update existing damages laws. To more broadly address AI-based harms, this 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.

### China

**Current Legislation**. At present, while China does not have a comprehensive approach to AI liability, AI is subject to liability. At the highest judicial levels, Chinese courts are taking interest in safeguarding individual rights against AI software-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 that infringed personality rights by using the portrait of a natural person without the person's consent.[70] 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 reflected a thoughtful exploration of standards for assessing AI algorithms and applications, and highlights the significance of protecting personality rights in the AI age.

### 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)[71] and the Product Liability Act (Act No. 85 of July 1, 1994).[72]

Similar to the current EU Product Liability Directive, the 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[73] and 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.

## CONCLUSION—KEY CONSIDERATIONS FOR THE PRIVATE SECTOR

For businesses, innovative development and deployment of AI poses tremendous opportunities but also risks. Navigating these opportunities and risks will require an eye to the evolving legal issues that AI poses. While each situation, product, and service will pose different questions, general recommendations for addressing the legal implications of AI include:

- **Keep abreast of the growing regulation of AI globally.** AI regulation is growing across the globe, and interest in AI oversight will expand more over time. When developing new AI systems, companies should anticipate constraints that 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 front-runner 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 just entering the field. Depending on its area of business, a company may find itself entering into 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 also 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 law.

- **Maintain privacy when personal data is concerned.** AI systems using personal data call for specific attention, as these are already covered by GDPR and other privacy legislations. The obligation to conduct an impact assessment, under GDPR and the forthcoming AI Act, should be considered. In the United States, companies can expect the implementation of a national data privacy regulation similar to the GDPR in the near-term future. As the number of states that pass their own data privacy legislation continues to increase along with growing calls to harmonize data privacy laws between the United States and European Union, a nationwide privacy regulation is becoming increasingly likely.
- **Monitor data flows.** Several regulations, like 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. 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.** Specific attention should be given to risks of biases triggered or amplified by the use of AI. 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 ensure any training data sets 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 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.
- **Manage liability risks.** Navigating multiple increasingly proscriptive, 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 ensure 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 identifying any 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.

With each of these issues, 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 has developed far enough, however, that AI can no longer be regarded as a purely technical issue confined to the realm of specialists—it is becoming a more mainstream issue for lawmakers, regulators, and practicing lawyers in a range of fields.

## 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.


**Laurent De Muyter**
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

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

**Carl A. Kukkonen III**
San Diego/Silicon Valley
+1.858.314.1178/+1.650.687.4178
ckukkonne@jonesday.com

**Alexander V. Maugeri**
New York
+1.212.326.3880
amaugeri@jonesday.com

**Schuyler J. Schouten**
San Diego/Washington
+1.858.314.1160/+1.202.879.3844
sschouten@jonesday.com

**Michiru Takahashi**
Tokyo
+81.3.6800.1821
mtakahashi@jonesday.com

**Olivier Haas**
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

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

**Matthew W. Johnson**
Pittsburgh
+1.412.394.9524
mwjohnson@jonesday.com

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

**Alexandre G. Verheyden**
Brussels
+32.2.645.15.09
averheyden@jonesday.com

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

## ENDNOTES

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2 European Parliament, Panel for the Future of Science and Technology, "Study: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence." (EPRS__STU(2020)641530) (June 2020).

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

4 Directive (EU) 2019/1024 of the European Parliament and of the Council of June 20, 2019, on open data and the reuse of public sector information (recast). As an EU directive (unlike a directly applicable EU regulation), the Open Data Directive required Member State transposition into national laws by July 16, 2021.

5 Communication from the Commission, "A European Strategy for Data."

6 Regulation EU 2022/868 of the European Parliament and of the Council on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

7 *See* Jones Day *Alert*, "European Commission Proposes Legislation Facilitating Data Access and Sharing" (Feb. 2022).

8 Directive (EU) 2015/2366. *See also* European Data Protection Board, "Guidelines 06/2020 on the interplay of the Second Payment Directive and the GDPR" (Dec. 15, 2020).

9 Directive 2019/944 of June 5, 2019, on common rules for the internal market for electricity; Directive 2009/73 of July 13, 2009, concerning common rules for the internal market in natural gas.

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

11 Regulation 2007/715, amended by Regulation 2018/858.

12 Directive 2010/40 of July 7, 2010, on the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other modes of transport. The Commission published a proposal for a revised ITS Directive in Dec. 2021.

13 The Commission launched a public consultation in March 2022 on the sharing of vehicle-generated data and is expected to publish an EU regulation on access to in-vehicle data in 2023.

14 Proposal for a Regulation on the deployment of alternative fuels infrastructure, July 14, 2021.

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

16 Proposal for a regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final.

17 *See* Draft Horizontal Guidelines, §442.

18 *See, e.g.*, Commission decision of June 30, 2022, in Case AT. 40511, 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.

19 *See, e.g.*, Commission decision of Dec. 20, 2012, in Case AT.39654, 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.

20 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.

21 "Personal Information Protection Law of the People's Republic of China" (available in Chinese only). *See also* "China to Start Implementing Restrictions on Cross-Border Transfers of Personal Information," Jones Day *Commentary* (Aug. 2022).

22 PIPL, Article 13.

23 PIPL, Article 24.

24 PRC Antitrust Law (2007), Article 9.

25 Measures for the Security Assessment of Outbound Data Transfer (2022), Article 4.

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

27 Significant amendments to the APPI were recently made in 2020 and 2021. The 2020 amendment in its entirety and the 2021 amendment (available in Japanese only) partially took effect on Apr. 1, 2022. The 2021 amendment will fully take effect on April 1, 2023 (available in Japanese only). An English translation is available only for the 2020 amendment of the APPI.

28 APPI, Article 21, Para. 1.

29 APPI, Article 27, Para. 1.

30 APPI, Article 28, Para 1.

31 APPI Article 28, Para. 2, APPI implementation regulation, Article 17, Para. 2.

32 "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 Article 2, Para. 2.

33 APPI Article 20, Para. 2.

34 APPI Article 27, Para. 2.

35 "Act on Anonymized Medical Data That Are Meant to Contribute to Research and Development in the Medical Field" (available in Japanese only).

36 Next Generation Medical Infrastructure Act, Article 30.

37 The most updated version is version 2.1, published in Aug. 2021 (available in Japanese only). The draft of version 2.2 was published for public comments on June 30, 2022 (available in Japanese only).

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

39 "Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Act No. 54 of April 14, 1947)."

40 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions, Artificial Intelligence for Europe, COM/2018/237 final.

41 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions fostering a European approach to artificial intelligence, COM(2021) 205 final.

42 Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts (com(2021) 206 final. The proposed AI Regulation is accompanied by a proposal for a new Regulation on Machinery Products, which focuses on the safe integration of an AI system into machinery.

43 Proposal for a Regulation of the European Parliament and of the Council on general product safety.

44 Directive 2001/95/EC of the European Parliament and of the Council of Dec. 3, 2001, on general product safety.

45 Regulation (EU) 2019/881 of the European Parliament and of the Council of Apr. 17, 2019, on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) NO 526/2013 (Cybersecurity Act).

46 Regulation (EU) 2017/745 of the European Parliament and of the Council of Apr. 5, 2017, on medical devices, amending Directive

2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No. 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

47 Regulation (EU) 2017/746 of the European Parliament and of the Council of Apr. 5, 2017, on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU.

48 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

49 "The State Council on Printing and Distributing Notice of the New Generation Artificial Intelligence Development Plan" (available in Chinese only).

50 "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'" (available in Chinese only).

51 "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).

52 Letter from the Ministry of Science and Technology on Supporting Harbin in Building a National New Generation Artificial Intelligence Innovation and Development Pilot Zone (2021); Letter from the Ministry of Science and Technology on Supporting Shenyang to Build a National New Generation Artificial Intelligence Innovation and Development Pilot Zone (2021); Letter from the Ministry of Science and Technology on Supporting Zhengzhou to Build a National New Generation Artificial Intelligence Innovation and Development Pilot Zone (2021).

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

54 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.

55 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.

56 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. Letter from the General Office of the Ministry of Housing and Urban-Rural Development on the approval of Beijing to carry out the pilot project of using artificial intelligence to review construction drawings (2020); Letter from the General Office of the Ministry of Housing and Urban-Rural Development on the approval of Shenzhen to carry out the pilot project of using artificial intelligence to review construction drawings (2020).

57 "Notice on Issuing the 'Guidelines for the Practice of Network Security Standards-Guidelines for Prevention of Artificial Intelligence Ethical Security Risks'" (available in Chinese only).

58 "AI Governance in Japan Ver. 1.1: Report from the Expert Group on How AI Principles Should Be Implemented," July 9, 2021.

59 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.

60 *See* AI Governance Guidelines, A. Introduction, 4. "How to Use the AI Governance Guidelines."

61 *Id.*

62 The Conference toward AI Network Society, "Draft AI R&D Guidelines for International Discussions" (July 28, 2017).

63 The Conference toward AI Network Society, "AI Utilization Guidelines Practical Reference For AI Utilization" (Aug. 9, 2019).

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

65 Council Directive 85/374/EEC.

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

67 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.

68 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.

69 Commission consultation, "Civil Liability–Adapting Liability Rules to the Digital Age and Artificial Intelligence."

70 "Nine Model Civil Cases of Judicial Protection of Personality Rights after the Issuance of the Civil Code Published by the Supreme People's Court (2022)" (available in Chinese only).

71 Civil Code (Part I, Part II, and Part III).

72 Product Liability Act (Act No. 85 of 1994).

73 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. (Article 2, para. 2).