

# AI in 2024: Monitoring New Regulation and Staying in Compliance With Existing Laws

## Contributing Partners

**Ken D. Kumayama** / Palo Alto

**Michael E. Leiter** / Washington, D.C.

**William Ridgway** / Chicago

**Resa K. Schlossberg** / New York

**David E. Schwartz** / New York

**David A. Simon** / Washington, D.C.

## Counsel

**Pramode Chiruvolu** / Palo Alto

**Eve-Christie Vermynck** / London

## Associate

**Lisa V. Zivkovic** / New York

### This article is from Skadden's 2024 Insights.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West  
New York, NY 10001  
212.735.3000

## Key Points

- AI regulation, including the EU's AI Act, is taking shape and may begin to affect nearly all industries.
- Expect more litigation over alleged copyright infringement in the training and use of AI systems.
- AI technology will increasingly generate cybersecurity challenges and privacy risks that companies utilizing AI systems must manage.
- The use of AI in employment decisions will be circumscribed by employment-related laws.
- As companies integrate AI into products and processes, robust internal governance policies will be needed to manage risks related to the use of proprietary and confidential information, as well as of customer and employee personal information for AI input, for example.

To stay in compliance with existing rules across jurisdictions and prepare for new ones in the making, companies will need to monitor regulatory developments and consider whether to submit comments or otherwise be involved in legislative or regulatory rulemaking on issues affecting their interests.

## 1. Upcoming AI Legislation

Governments across the world have only just begun to draft and pass laws tailored to AI technology. Heading into 2024, we expect both sector-specific and broader, omnibus AI regulations to impact nearly all industries as the use of AI expands.

### European Union

The EU set rules for the use of AI, namely the EU Artificial Intelligence Act (EU AI Act) and the Artificial Intelligence Liability Directive (AILD).

**EU AI Act.** On December 8, 2023, EU policymakers reached a deal on the EU AI Act following three days of marathon negotiations. The EU AI Act still needs to go through final steps before it becomes law, but the political accord means that its key parameters have been set. The provisional agreement provides that the EU AI Act will apply two years after its entry into force, with some exceptions

for specific provisions. The draft law needs the approval of the Council of the European Union and the European Parliament, which comprises representatives from the 27 countries in the EU.

The legislation, which would apply to providers placing AI systems in the EU market, would take a "risk-based" approach, classifying and regulating systems based on their risk levels. For example, new provisions were introduced to account for general purpose AI systems, to require specific transparency obligations for foundational models before being placed on the market, and to impose a stricter regime for high-impact foundational models.

The legislation, which would apply to providers placing AI systems in the EU market, would take a "risk-based" approach, classifying and regulating systems based on their risk levels.

The draft law also deems risks associated with certain use cases unacceptable, banning, for example, the scraping of faces from the internet or security footage to create facial recognition databases;

emotion recognition in the workplace and educational institutions; cognitive behavioral manipulation; social scoring; biometric categorization to infer sensitive data, such as sexual orientation or religious beliefs; and certain cases of predictive policing for individuals. However, the draft law also gives broad exemptions for “open-source models.”

The draft law specifies that the scope of the law shall not affect member states’ competences in national security (or any entity entrusted with tasks in this area) or apply to AI systems used solely for the purpose of research and innovation.

**AILD.** In parallel, the EU is amending its product liability regime, updating the existing Product Liability Directive and adopting the new AILD to harmonize civil liability for AI among EU member states.

The amendments would address strict and fault-based liability regimes to provide recourse to EU citizens for defective or harmful AI products. Importantly, the AILD would establish a rebuttable presumption of a causal link between the fault of the provider of AI systems and the output of those systems.

These regimes will not only affect companies looking to launch and use AI models in the EU but may also help shape future legislation by EU member states and other jurisdictions.

### United Kingdom

In contrast, the U.K. has taken an incremental, sector-led approach to AI regulation, as reflected in its [March 2023 white paper](#). The U.K. government has undertaken consultations and invited feedback from the AI industry to guide its regulation of AI practices. In the coming year, it is expected to share high-level guidance and an initial regulatory road map with its sector-specific regulators.

These regulators will then provide tailored recommendations for the financial, health care, competition and employment sectors. At that point, the U.K. government will assess whether specific AI regulation, or an AI regulator, is required, which will inform the business practices of companies placing AI systems in the U.K. in 2024.

### United States

The U.S. has yet to adopt a comprehensive AI law. However, in October 2023, the Biden administration issued a [sweeping executive order](#) (AI Executive Order) that directed various U.S. government departments and agencies to evaluate the safety and security of AI technology and other associated risks, and implement processes and procedures regarding the adoption and use of AI. Federal and state agencies as well as lawmakers have also shown significant interest in regulating AI technology.

**AI Executive Order.** The executive order set deadlines for agencies and regulators, and proposed to impose obligations on companies to test and report on AI systems. It followed a suite of AI policies that the White House announced earlier in 2023. (For more on the executive order, see our November 3, 2023, client alert “[Biden Administration Passes Sweeping Executive Order on Artificial Intelligence](#).”) Heading into the new year, we expect accelerated efforts to enact AI regulation, particularly in light of the AI Executive Order, both at the federal and state levels.

**CPPA’s proposed regulations on automated decision-making.** The California Privacy Protection Agency (CPPA) recently issued an initial draft of regulations governing the use of automated decision-making technology (ADMT) under the California Consumer Privacy Act (CCPA). The draft regulations broadly define any system, software or process that handles the personal

information of California residents and uses computation as a whole or part of a system to make or execute a decision or facilitate human decision-making.

The draft regulations propose granting consumers (including employees and business-to-business contacts) the right to receive pre-use notice regarding the use of ADMT and to opt out of certain automated decision-making activities. The CPPA is expected to begin the formal rulemaking process in 2024.

**Copyright Office and Patent and Trademark Office.** The two agencies have issued enforcement actions and guidance on various AI-related matters, taking the position that a sufficient degree of human input is needed to qualify for protections under copyright and patent law. Subsequent litigation has affirmed these positions. (See our August 28, 2023, client alert “[District Court Affirms Human Authorship Requirement for the Copyrightability of Autonomously Generated AI Works](#).”) We expect guidance from the two agencies to evolve as applicants seek to register new works and inventions that incorporate AI in 2024.

**SEC’s proposed AI rules.** In July 2023, the Securities and Exchange Commission (SEC) proposed broad new rules to address conflicts of interest that the SEC believes are posed by the use of AI and other types of analytical technologies by broker-dealers and investment advisers. We expect the final rules to be released in 2024. (See our August 10, 2023, client alert “[SEC Proposes New Conflicts of Interest Rule for Use of AI by Broker-Dealers and Investment Advisers](#).”)

### Other Jurisdictions

Beyond the EU and U.S., more than 37 countries — including China, India and Japan — have proposed AI-related legal frameworks.

- In August 2023, the International Association of Privacy Professionals published [a list of AI legislation introduced around the world](#).
- In October 2023, the United Nations unveiled an AI advisory board aimed at creating global agreements on how to govern AI systems. The board plans to release final recommendations by mid-2024, which may influence worldwide regulatory efforts.
- On November 1, 2023, representatives from the EU, U.S., U.K., China and 25 other countries signed the Bletchley Declaration, largely echoing the statements of numerous national and international organizations in recognizing the importance of trustworthy AI and the potential dangers of general-purpose AI models. The declaration suggests international cooperation and an inclusive global dialogue that recognizes varying approaches based on national circumstances.

## 2. Current and Future Litigation Copyright Infringement

Generative AI models, including ChatGPT and Google Bard, are generally trained on vast amounts of content and data. These may include copyrighted works extracted from publicly available websites. A number of content creators and owners have filed suits claiming that use of this content infringes the rights, including copyrights, of third parties.

Data compilers and model trainers have argued that their activities constitute “fair use” under copyright law. These cases are just beginning to work their way through the courts.

Cases to watch include:

- *Thomson Reuters v. ROSS Intelligence*: Legal publisher alleges infringement of copyrights in Westlaw material used to train an AI-based competitor.
- *Getty Images v. Stability AI*: Image licensor alleges infringement of copyrights in over 12 million photos and their captions used to build and promote the text-to-image generative AI systems Stable Diffusion and DreamStudio.
- *Authors Guild v. OpenAI Inc.*: Novelists in putative class action accuse OpenAI of using their works without permission to train the AI models powering ChatGPT.
- *Tremblay/Silverman v. OpenAI Inc.*: Two plaintiff groups allege that OpenAI infringed their copyrighted novels to train the AI models powering ChatGPT.
- *Doe v. GitHub Inc.*: Software developers allege that the AI-based coding tools OpenAI Codex and GitHub Copilot infringed rights and violated licensing terms relating to public code developers published on GitHub.

## 3. Cybersecurity and Privacy Risks

### Cybersecurity

AI technology has the capability to expand the arsenal of bad actors to carry out sophisticated cyberattacks (e.g., large language models can be used to write malicious code, engineer advanced phishing attacks or more effectively spread malware and ransomware). In addition, AI systems may themselves be vulnerable to data integrity attacks (e.g., through “model poisoning,” an attack conducted by introducing malicious information into training data).

In response to those risks, the AI Executive Order in the U.S. calls for testing and reporting rules for companies developing certain AI tools. Companies must therefore ensure their cybersecurity polices adequately identify, measure and manage these risks.

### Privacy

Companies that build or use AI models built on training sets that include personal information — whether purchased from third parties or extracted from publicly

available websites — or that otherwise collect personal information, including through inputs by users (such as through note-taking and summarization technologies built into web conferencing software), may implicate privacy laws in various jurisdictions.

**Applicability of comprehensive privacy laws.** Comprehensive privacy laws, such as the EU’s General Data Protection Regulation (GDPR), the CCPA and other U.S. state privacy laws, impose purpose limitation, data minimization, transparency, accountability and integrity principles that may be at odds with the use and development of such AI models. Therefore, companies will need to carefully consider whether they are providing individuals whose personal information is used for or by AI models with the requisite notices and are obtaining the necessary consent prior to such use. Companies will also need to be prepared to respond to requests by these individuals to exercise their rights — some of which, such as the right to delete, are complicated by the mechanisms of AI — under the privacy laws.

### Lawsuits under biometric privacy laws.

AI companies have faced suits under the Illinois’ Biometric Information Privacy Act, which prohibits private companies from collecting biometric data unless they follow stringent requirements. For example, recent lawsuits in state courts allege Clearview AI scraped billions of pictures from social media platforms to create a faceprint database that was then sold to police departments and other private organizations.

**FTC’s asserted authority over AI.** The Federal Trade Commission (FTC) has enforced the FTC Act’s prohibitions on unfair and deceptive acts or practices against AI companies (including requiring in some cases that AI models trained on data in violation of privacy commitments be deleted, a remedy termed “algorithmic disgorgement”). The FTC has also

indicated that it will continue to enforce the FTC Act to protect against misuses of personal information in connection with AI models. (See “[FTC Enforcement Trends in Consumer Protection Under the Biden Administration](#).”)

In addition, the FTC recently approved, in a 3-0 vote, a resolution authorizing its ability to issue civil investigative demands (CIDs), which are a form of compulsory process similar to a subpoena, in non-public investigations involving products and services that use or claim to use AI.

#### 4. Labor and Employment Issues

Many companies are already harnessing AI to improve efficiency in employment processes by, for example, preparing job descriptions, screening and evaluating job candidates, and analyzing data to predict the future success of job applicants. AI may also be used to analyze employee productivity, measure performance and identify candidates for promotion.

##### Hiring and Promotion

An employer’s use of AI in hiring and promotion must comply with laws that prohibit discrimination based on race, color, religion, sex, national origin, disability or age, including Title VII of the Civil Rights Act of 1964, the Americans With Disabilities Act and the Age Discrimination in Employment Act in the U.S.

In 2022 and 2023, the U.S. Equal Employment Opportunity Commission (EEOC) [issued guidance with examples of ways that AI tools may violate anti-discrimination laws](#) and best practices to employ when integrating AI into HR policies and practices.

In addition, state and local legislators are focused on AI use in hiring and promotion. For example, New York City Local Law 144 requires employers using automated employment decision tools (AEDTs) to screen candidates for hiring or promotion to make public the date and summary of the results of an annual independent bias audit of any such AEDTs.

Illinois also enacted the Artificial Intelligence Video Interview Act in 2022, which imposes certain requirements on employers that use AI to analyze video interviews. California, New Jersey, New York, Vermont and Washington, D.C., have also proposed legislation to regulate AI use in hiring and promotion.

In addition, employers and employment agencies must provide a notice of the use of AEDTs to employees and candidates for employment who reside in New York City.

##### Termination

When laying off employees, employers must also be mindful of compliance not only with anti-discrimination laws but also the U.S. Worker Adjustment and Retraining Notification Act and equivalent state and local laws. Furthermore, pending legislation may impact employers; for example, the U.S. Algorithmic Accountability Act of 2022 would direct the FTC to require organizations to conduct impact assessments for bias when using AI systems to make critical decisions, such as whom to lay off. (See our June 2023 article “[AI and the Workplace: Employment Considerations](#).”)

#### 5. AI Governance Practices

As AI becomes integrated more broadly into products and business practices, and as regulations affecting AI use take

shape, companies should implement — and regularly update — clear and robust internal governance policies in order to minimize risk and liability.

Specifically, heading into 2024, companies should consider:

- **Terms of use.** Ensure public-facing terms of use sufficiently reflect internal policies regarding AI. For example, companies that make valuable intellectual property (IP) available on their websites should draft terms that make it clear whether use of that IP in connection with third-party AI products is prohibited.
- **Employee policies.** Outline the scope of permitted use of AI in the workplace in internal policies, and design protections for the use of confidential information or IP as inputs in AI tools, as well as processes governing the use of AI-generated content in products and services.
- **Vendor agreements.** Develop and implement policies and processes to address any AI-specific risks arising from their vendor agreements and ensure that negotiated agreements have sufficient protections regarding the use of confidential, proprietary or personally identifiable information, IP infringement risks and IP ownership.
- **Updating processes to reflect AI risks.** Integrate AI-related risks into compliance and governance processes, including through assessments of the impact of AI-related development or procurement, and through training and tabletop exercises to sensitize employees, management and boards to key AI issues likely to affect the organization.