The AI Regulatory Puzzle — from the EU to the U.S.

While artificial intelligence (AI) has been around for many years, the technology has exploded in both its use and development across virtually all industries in recent years. Although AI has the potential to be used in innovative and positive ways, it also can be used to perpetrate fraud and crime, cause discrimination and bias, promote and disseminate disinformation, violate personal privacy, and threaten national security. Thus, the rapid growth of AI technology and its associated risks has created an urgent need for regulation.

Similar to data privacy laws, the European Union (EU) has led the way in efforts to regulate AI. In the U.S., there is no uniform federal law regulating AI nor is any such framework on the horizon. Thus, in addition to data privacy laws that apply to AI, individual state and local governments have begun enacting laws and regulations specifically addressing AI systems. These various laws, which differ in applicability and scope, create the possibility of there being a patchwork of overlapping and conflicting regulations and laws. It is important that entities doing business in the U.S. be vigilant about the various AI laws that may be applicable and ensure compliance. This advisory is intended to provide a broad summary of the AI regulatory landscape.

European Union AI Act

The EU's Artificial Intelligence Act (the EU AI Act) was the first comprehensive legal framework for the regulation of AI systems, and is already becoming a model for other jurisdictions.[1] It went into effect across all EU Member States on August 1, 2024, and the enforcement of the majority of its provisions will begin on August 2, 2026.

It applies to any AI System which is defined as "a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." The EU AI Act applies to providers, developers, importers, and users/deployers who place or put into service AI systems in the EU market, irrespective of where they are established or located, but does not apply to AI systems used solely for scientific research, development, and testing.

The EU AI Act features a risk-based approach to regulation which requires an initial assessment of the risks each AI system can generate. The EU AI Act completely bans certain AI practices that present an unacceptable risk to fundamental rights, such as those that manipulate human behavior or exploit individuals' vulnerabilities (e.g., age or disabilities). High-Risk AI systems are the most highly regulated and include AI systems used in critical infrastructures, in medical devices and safety products, and in ways that affect access to educational and employment opportunities. The EU AI Act imposes a wide range of obligations on entities using high-risk AI systems, including implementation of a risk management program, data training and data governance, technical documentation, recordkeeping, transparency, human oversight, and cybersecurity. High-risk AI systems also must be registered in an EU database before such AI systems are released in the EU market, thus the assessment of whether an AI system is high-risk must be done in advance.

Limited-risk AI systems, such as chatbots, must merely ensure that users are provided notice that they are interacting with an AI system. There are no restrictions on minimal-risk AI systems, such as spam

filters or video games. Penalties for non-compliance include a maximum financial penalty of up to EUR 35 million or seven percent (7%) of worldwide annual turnover, whichever is greater.

U.S. — Federal

While there currently is no comprehensive federal law regulating the use of AI, various federal agencies have issued pronouncements, frameworks, and guidelines on the subject of AI.

In October 2022, the White House Office of Science and Technology Policy (OSTP) issued an AI Bill of Rights, which essentially is a set of guidelines for the responsible design and use of AI and the result of collaboration between the OSTP, academics, human rights groups, nonprofits, and large technology companies.[2]

In October 2023, building off the AI Bill of Rights, the White House issued an Executive Order entitled "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" which directs federal agencies to develop standards and regulations that will allow for the responsible use and expansion of AI while mitigating its risks.[3]

In May 2023, the Equal Employment Opportunity Commission issued guidance concerning employers' use of AI tools, making clear that employers may be held responsible for using AI in a manner that has an adverse or disparate impact on people in a protected class.[4]

Several other agencies, including the Department of Commerce, National Institute of Standards and Technology, Department of Defense, Department of Homeland Security, Department of Energy, Department of Labor and others have issued guidelines or draft rules on AI.

U.S. States — Comprehensive AI Laws

As occurred with data privacy regulations, individual U.S. states have begun enacting AI legislation to fill the void caused by the lack of a federal framework.

Utah

Utah became the first U.S. state to enact a broad statute specifically governing AI. The Utah Artificial Intelligence Policy Act (AIPA), which became effective May 1, 2024, regulates the use of Generative AI ("Gen AI") technologies by businesses or individuals to interact with Utah consumers.[5]

Gen AI is AI used to interact with persons using text, audio, or visual communication. When a business or person uses Gen AI to interact with an individual, they are required to disclose that the individual is interacting with Gen AI if the individual asks.

If Gen AI is used in providing services of "regulated occupations" (those that require a license or state certification, such as accountants and physicians), a prominent mandatory disclosure must be clearly and conspicuously provided.

The Utah Division of Consumer Protection may impose a fine of up to $2,500 per violation; there is no private right of action.

The AIPA also creates a new AI regulatory body, the Office of Artificial Intelligence Policy, tasked with establishing an AI "Learning Laboratory Program" which will assist with analyzing risks and benefits and will allow participants to test and develop AI technology with limitations on liability.

Colorado

In May 2024, Colorado enacted its own comprehensive AI regulation, the Colorado AI Act, which will become effective on February 1, 2026.[6] Colorado's AI Act, like the EU AI Act, adopts a risk-based

approach to AI regulation, and applies to developers and users of AI systems who are doing business in Colorado.

It imposes notice, documentation, disclosure, and impact assessment requirements on developers and deployers of any "high-risk" AI system, defined as an AI system that "makes, or is a substantial factor in making, a consequential decision" (i.e., any decision that "has a material legal or similarly significant effect on the provision or denial to any consumer, or the cost or terms, of" education or employment opportunities, financial or lending services, essential government services, healthcare services, housing, insurance, or legal services).

It requires that developers and entities that deploy "high-risk" AI systems use reasonable care to prevent algorithmic discrimination. There is a rebuttable presumption that reasonable care was used if they meet certain requirements, such as having a risk management policy and program, and providing notice to consumers of the use of AI in making a consequential decision and notice of consumer rights (such as the right to correct inaccurate personal data and the right to appeal a decision).

Colorado's Attorney General has exclusive authority to enforce the Colorado AI Act and issue penalties of up to $20,000 per violation. There is no private right of action.

California

On September 19, 2024, California enacted the California AI Transparency Act, which goes into effect January 1, 2026.[7]

It will require providers of Gen AI systems to make available an AI detection tool, at no cost to users, that will allow users to check whether images, video, or audio content has been created or altered using a Gen AI system. Providers must include latent disclosure in AI-generated content (i.e., in metadata) that can be detectable using the AI detection tool. Also, users must be provided the option of having a manifest disclosure, clearly conveying that content is AI generated. Providers that license their Gen AI systems to third parties must have agreements with the licensees requiring that they maintain these disclosure requirements. If covered providers know that third-party licensees are not capable of including such disclosures, they will be required to revoke their licenses within 96 hours.

It applies to any "covered provider," defined to mean "a person that creates, codes, or otherwise produces a generative artificial intelligence system that has over 1,000,000 monthly visitors or users and is publicly accessible" within California.

It will be enforced by the California Attorney General, a city attorney, or a county counsel, and provides for civil penalties of $5,000 per day.

Also, in September 2024, California enacted several other AI-related laws in various areas, including health care, data privacy, watermarking content (provenance data), robocalls, deepfake pornography, election deepfakes, and entertainment industry use of voice or likeness replicas.[8]

Other States

Many other states have proposed similar legislation, and it is expected that 2025 will see more states enact comprehensive AI laws.

AI Laws in Employment Context

Those that use AI technology in employment-related decisions are subject to some of the above-referenced laws but also certain employment-specific laws enacted by U.S. states and cities. Regulators are seeking to prevent the use of AI algorithmic systems that make decisions about candidates based on factors like race, ethnicity, and gender. Many companies use AI systems in screening resumes and

sorting and analyzing employment applications, in some cases with the systems predicting the success of candidates based on individual characteristics.

New York City enacted the first employment-specific AI law in the U.S., which became effective in July 2023.[9] As discussed in our July 2023 advisory, it requires employers or employment agencies that use automated employment decision tools (AEDTs), located in New York City or involving NYC employees, to submit those AEDTs to periodic bias audits, to make information about the bias audit publicly available, and to provide certain notices to job candidates or employees. An AEDT is defined as technology that "is used to substantially assist or replace discretionary decision making" in hiring or other employment-related decisions by relying on factors generated by a machine (likely using artificial intelligence algorithms). Employers and employment agencies who use AEDTs must adhere to audit and disclosure requirements. Failure to do so runs the risk of enforcement actions.

In August 2024, Illinois enacted a law that will go into effect on January 1, 2026.[10] Under this law, employers will be required to notify employees when they use AI for employment decisions which include recruitment, hiring, promotion, renewal of employment, selection for training, discharge, discipline, tenure, or the terms, or conditions of employment. It prohibits employers from using AI in a manner that discriminates against employees that are within protected classes in Illinois. Illinois also has a law, which took effect in January 2020, that requires employers who use AI to analyze video interviews of applicants to, among other things, provide notice and obtain consent.

Other states have also introduced bills to specifically regulate the use of AI in the employment context, while several state privacy laws currently in effect also provide some overlapping coverage, as discussed below.

In addition, employers may be subject to liability under long-standing federal discrimination laws, such as Title VII of the Civil Rights Act of 1964 (Title VII), if their use of AI leads to discrimination or disparate impacts on protected classes of people, as discussed in our July 2024 advisory.

State Data Privacy Laws

Often overlooked is the fact that many existing state data privacy laws have AI regulation components. Specifically, such laws regulate the use of automated decision-making technology (ADMT) in processing personal data. ADMT generally refers to the use of automated processes with personal data to make decisions around financial or lending services, housing, insurance, educational enrollment, criminal justice, employment opportunities, health care services or access to essential goods or services. Common examples include the use of AI to process personal data in connection with determining loan qualifications or in hiring and employment decisions (like AEDT described above). Profiling generally means the automated processing of personal information to assess and predict a person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. A common example of AI-related profiling is the widespread use of targeted advertising by websites. In general, state privacy laws require notice to consumers and the opportunity for consumers to opt out of such processing of their personal data in these contexts.

States with currently effective data privacy laws that regulate the use of AI technology, such as ADMT, involving personal data include California, Colorado, Connecticut, Virginia, Utah, Texas, Oregon, and Montana. Other states have similar laws that will go into effect in 2025.

Takeaways

Given the various laws applicable to AI that are currently in effect and those on the way, and the somewhat uncertain regulatory future, it is important that companies immediately assess their use of AI and evaluate their compliance obligations. Once an organization has mapped its AI uses, it should assess what laws may be applicable and develop programs for compliance. Organizations should consider whether to address AI uses in its privacy policies and terms of use, employee manuals and policies, vendor agreements, and information security programs. And, of course, organizations should continue to closely monitor regulatory developments.

This article was written by Matthew D. Dunn (212-238-8706, mdunn@clm.com) of Carter Ledyard & Milburn LLP.

[1] Council Regulation (EU) 2024/1689 (amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act)) (June 13, 2024), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

[2] Blueprint for an AI Bill of Rights, White House Off. of Sci. & Tech, Pol'y (last visited Nov. 7, 2024), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[3] Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75, 191, EO 14110 (Nov. 1, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[4] Title VII and AI: Assessing Adverse Impact, U.S. EEOC, Title VII, 29 C.F.R. Part 1607 (May 18, 2023), https://www.eeoc.gov/laws/guidance/select-issues-assessing-adverse-impact-software-algorithms-and-artificial.

[5] https://le.utah.gov/~2024/bills/static/SB0149.html

[6] Consumer Protections for Artificial Intelligence, S. 205, 74th Gen. Assembly 2nd Regular Session (2024), https://leg.colorado.gov/bills/sb24-205.

[7] California AI Transparency Act, Sen. 942, Ch. 291 (adding Ch. 25, Sec. 22757 to Div. 8 of Bus. & Prof. Code) (2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942#:~:text=This%20bill%2C%20the%20California%20AI,detection%20tool%20is%20publicly%20accessible

[8] Governor Newsom announces new initiatives to advance safe and responsible AI, protect Californians, Governor Gavin Newsom (Sept. 29, 2024), https://www.gov.ca.gov/2024/09/29/governor-newsom-announces-new-initiatives-to-advance-safe-and-responsible-ai-protect-californians/.

[9] Automated Employment Decision Tools (AEDT), NYC Consumer & Worker Protection (last visited Nov. 8, 2024), https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page.

[10] Limit Predictive Analytics Use, HB 3773, 103rd General Assembly (Ill. Pub. Act 103-0804) (2024), https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3773&GAID=17&DocTypeID=HB&SessionID=112&GA=103.

***