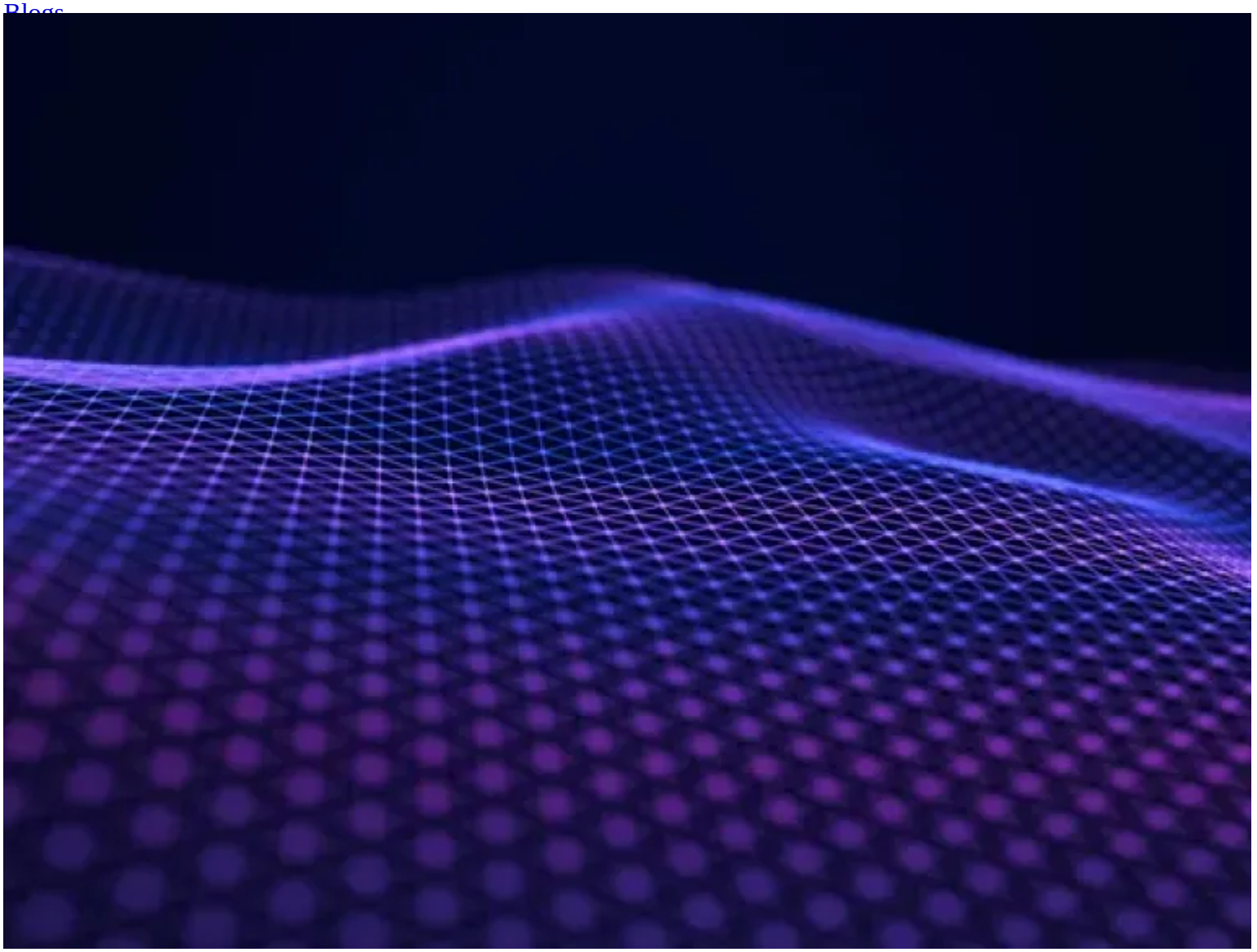

The European Union seized the early global lead in regulating artificial intelligence (AI) by passing its AI Act on March 13, 2024, following a lengthy legislative process.[1] Meanwhile, across the Atlantic, the U.S. Congress has made noise about the need for federal AI legislation, but progress has been slow. The absence of a similarly comprehensive federal law from Congress has created a vacuum that is now being filled by individual states.

These events are unfolding in a familiar pattern, reminiscent of what happened following the E.U. enactment of the General Data Protection Regulation (GDPR). While the GDPR became an international standard, the federal government failed to adopt a nationwide privacy law. States like California took the initiative to pass their own privacy laws, often drawing inspiration from the GDPR.

This Update summarizes recent U.S. state efforts to enact AI legislation, including the following:

- Most recently, on May 17, Colorado Governor Jared Polis signed into law a bill concerning "Consumer Protections in Interactions with Artificial Intelligence," which provides a risk-based AI regulatory framework similar to the E.U. AI Act. Meanwhile, Connecticut failed to pass an AI law similar to Colorado's. Connecticut Governor Ned Lamont threatened to veto the law if it had been passed, arguing that Connecticut was better off working with a consortium of other states to address AI development and deployment across the private sector.
- In April, Utah enacted the "Artificial Intelligence Amendments," an AI-focused consumer protection bill that includes certain disclosure obligations where a person "uses, prompts, or otherwise causes generative artificial intelligence to interact with a person."
- In March, Tennessee enacted the "Ensuring Likeness, Voice, and Image Security (ELVIS) Act of 2024" to combat the rise of AI-generated voices and fake recordings (commonly known as "deepfakes").

Colorado: Consumer Protections in Interactions With Artificial Intelligence Systems

On May 17, 2024, Colorado enacted a new law concerning "Consumer Protections in Interactions with Artificial Intelligence Systems" (the Colorado AI Act). The law takes effect on February 1, 2026.

Similar to the E.U. AI Act, the Colorado AI Act adopts a risk-based approach to AI regulation by imposing certain notice, documentation, disclosure, and impact assessment requirements on developers and deployers of "high-risk" AI systems, which are defined to mean any AI system that "makes, or is a substantial factor in making, a consequential decision." The Colorado AI Act defines a "consequential decision" to mean 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, employment, financial, or lending services essential government services, healthcare services, housing, insurance, or legal services. As a result, the implications of the new law should be considered by a significant number of industries across the state.[2]

The Colorado AI Act focuses primarily on consumer protection, requiring developers and deployers of high-risk AI systems to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from the use of high-risk AI systems. The new law defines "algorithmic discrimination" to mean any condition in which the use of an AI system results in "an unlawful differential treatment or impact that disfavors an individual or group of individuals" on the basis of their age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under Colorado or federal law.

Colorado's attorney general has exclusive authority to enforce the Colorado AI Act, which expressly excludes any private right of action. Any violation of the Colorado AI Act would constitute a deceptive trade practice. However, developers and deployers would have a rebuttable presumption if they establish compliance with the law's requirements and an affirmative defense if they take certain steps to mitigate a violation of the law.

Colorado's new law comes on the heels of an AI regulatory bill that failed to pass in Connecticut. There, the state senate passed a bill substantially similar to the Colorado AI Act, but it died in the state's house of representatives following public statements from Connecticut's governor that he would veto the bill. In Colorado, the new law faced significant opposition from industry. Although Colorado's governor signed the bill into law, he took the extra step of writing a letter to lawmakers about his reservations. In his letter, Governor Polis expressed appreciation for the bill's "interest in preventing discrimination and prioritizing consumer protection," though he also emphasized that the new law should be improved upon before taking effect. For instance, while laws that seek to prevent discrimination generally focus on prohibiting intentional discriminatory conduct, this bill

deviates from that practice by regulating the results of AI system use, regardless of intent; Governor Polis encouraged the Colorado legislature to reexamine this concept as the law is finalized before it takes effect in 2026.

Utah: Artificial Intelligence Policy Act

Utah's AI Policy Act went into effect on May 1, 2024. The AI Policy Act includes disclosure obligations whenever someone causes generative AI "to interact with a person" in connection with laws administered and enforced by Utah's Division of Consumer Protection. Specifically, those providing generative AI must "clearly and conspicuously" disclose that the other person is interacting with generative AI, not a human, if that person asks. Further, anyone who provides services of an occupation regulated by the U.S. Department of Commerce that requires a license or state certification must disclose that the other person is interacting with generative AI at the beginning of a verbal of written exchange.

Tennessee: The Ensuring Likeness, Voice, and Image Security (ELVIS) Act

The ELVIS Act takes effect on July 1, 2024. It expands Tennessee's right of publicity law, providing that every individual has a property right in the use of their own name, photograph, likeness, or voice. These rights are exclusive to the individual during their lifetime and for 10 years after their death, with the rights then transferring to their executors, heirs, assigns, or devisees.

The ELVIS Act also creates private rights of action for unauthorized commercial use of an individual's name, photograph, likeness, or voice. Notably, it prohibits both knowingly making available a person's voice or likeness to the public without authorization and making available a technology, service, or device "the primary purpose or function of which is the production of an individual's photograph, voice, or likeness without authorization." Chancery and circuit courts may grant injunctions on terms they deem reasonable to prevent or restrain such unauthorized uses.

There are some "fair use" exceptions under the ELVIS Act for the unauthorized use of an individual's name, photograph, likeness, or voice. This includes use of those qualities in connection with a news, public affairs, or sports broadcast or account to the extent that use is protected under the First Amendment of the U.S.

California: Regulatory Enforcement

The California Civil Rights Council recently proposed regulations to protect against potential discrimination in hiring decisions resulting from use of AI and other automated systems.

In addition, California's Consumer Privacy Protection Agency continues to develop regulations related to automated decision-making technology, having last released a draft version at its board meeting in early March. The agency is now in the process of hosting pre-rulemaking stakeholder sessions (scheduled through May) to receive feedback on its proposals. At a high level, these draft regulations would implement a consumer's right to opt out of, and access information about, a business's use of automated decision-making technology. The draft regulations also would require a business to provide pre-use notifications to consumers, under certain circumstances, regarding how the business proposes to use automated decision-making technology.

Takeaways

Overall, AI regulations at the state level remain unsettled, with some states pushing forward with regulatory regimes tailored toward their specific concerns. In this context, Colorado's approach to AI regulation stands out as the most comprehensive and risk-based effort in the United States, resembling the E.U. AI Act.

Colorado's efforts initially suggest AI regulation may follow a similar path as consumer privacy laws, with proactive states taking inspiration from a comprehensive E.U. regulation (*i.e.*, the GDPR for privacy protection and the E.U. AI Act for AI regulation), while the U.S. Congress fails to act. On the other hand, Connecticut's failure to pass a similar bill inspired by the E.U. AI Act suggests that perhaps not all states will follow Colorado's lead. The mixed record of the state legislatures occurs amid the backdrop of little federal level activity aside from the executive branch, wherein the White House issued an expansive Executive Order last fall concerning the safe, secure, and trustworthy development and use of AI, which federal agencies have begun to implement.

Ultimately, states may face challenges passing comprehensive AI regulations due to AI developers' concerns about prematurely regulating a nascent industry and potentially stifling innovation. Either way, the AI regulation in the United States is relatively unsettled compared to the European Union and likely will remain so in the absence of federal legislation specifically addressing AI.

Endnotes

[1] On May 21, 2024, the Council of the E.U. approved the E.U. AI Act, providing the final green light to the world's first comprehensive regulation of AI. The E.U. AI Act will be published in the E.U.'s *Official Journal* in the coming days (after being signed by the presidents of the European Parliament and the Council) and enter into force 20 days after this publication; it will apply two years after its entry into force, with some exceptions for specific provisions.

[2] Certain technologies (unless deployed to make a consequential decision) are excluded from the definition of "high-risk" AI systems. These technologies include anti-fraud, anti-malware, and anti-virus technologies; AI-enabled video games; and databases and data storage, among others. Additionally, "technology that communicates with consumers in a natural language for the purpose of providing users with information, making referrals or recommendations, and answering questions and is subject to an acceptable use policy that prohibits generating content that is discriminatory or harmful" is also excluded. This would appear to exclude popular chatbots, such as those that use generative AI, although many terms used in this exclusion remain undefined (*e.g.*, "natural language," "making referrals or recommendations," and "answering questions").

Blog series

Age of Disruption

We live in a disruptive age, with ever-accelerating advances in technology largely fueling the disruption permeating almost every aspect of our lives.

We created the *Age of Disruption* blog with the goal of exploring the emerging technologies reshaping society and the business and legal considerations that they raise. Subscribe ?

View the blog