



Alerts

Strategic Artificial Intelligence Planning Alert: A State and Federal Regulatory Roadmap for 2025 Compliance

February 20, 2025

Privacy, Cyber & AI Decoded

The [World Economic Forum](#) has stated that 88 percent of C-suite executives indicated that adopting artificial intelligence (AI) in their companies is a key initiative for 2025.

Companies are pivoting from merely testing AI to expanding AI use cases in their business processes. While these new use cases can bring significant business benefits, they also introduce real contractual and legal risks that should be thoughtfully considered and potentially mitigated.

To help you reduce the barriers of using AI and also understand the legal risks involved, Hinshaw's Privacy, Security, & Artificial Intelligence team has prepared this Strategic AI Planning Alert for 2025. Keep reading to learn about key AI laws, legislation, guidance, and orders that may impact your organization's AI governance and use.

California

AB 1008: Amends the California Consumer Privacy Act Definition of "Personal Data" to Include AI *(Effective January 1, 2025)*

- Governor Newsom signed AB 1008 on September 28, 2024, which included AI systems capable of outputting personal information in the California Consumer Privacy Act's definition of personal information.
- This seemingly small change brings AI systems into the Act's requirements of notice, consent, data subject rights, and reasonable security controls.

SB 942: California AI Transparency Act *(Effective January 1, 2026)*

- On September 19, 2024, Governor Gavin Newsom signed into law the California AI Transparency Act, which requires covered providers to make disclosures about the use of generative AI systems concerning AI-generated content. This AI disclosure law will particularly impact all generative AI publishers, advertising agencies, and creators.
- If you are a covered provider, you must make available a tool to assess AI-generated content or include a conspicuous or "manifest" disclosure that it

Attorneys

Omar Mulamekic

Cathy Mulrow-Peattie

J. Michael Paulino

Claire Standish

Service Areas

Privacy, Security & Artificial Intelligence



is AI-generated content. This disclosure must be easily perceived, understood, and recognized by a natural person.

- SB 942 also requires that covered providers mark their AI-generated images with a "latent disclosure" created by the AI system that is permanent, detectable by the AI detection tool, and consistent with industry standards.
 - This latent disclosure must contain the name of the covered provider, the name and version number of the generative AI system that created or altered the content, a time and date stamp of the creation, and a unique image identifier.
 - This "latent disclosure" can either be on the image or linkable to a "permanent website." In your contract or license of these generative AI images, you must require your client to maintain this latent disclosure.

AB 2013: Requires Generative AI Training Data Documentation *(Effective January 1, 2026)*

- AB 2013 requires that a developer of a generative AI system or service, released on or after January 1, 2022, and which is made available to Californians for use, post on the developer's internet website documentation information about the data used to train the generative AI system or service.
- The law requires that this documentation includes, among other requirements, a high-level summary of the data sets used in developing the AI system or service.

Colorado

Colorado Artificial Intelligence Act *(Effective February 1, 2026)*

- The Colorado Artificial Intelligence Act (CAIA) has been compared to the European Union's (EU) AI Act. This Act applies to companies considered deployers and developers under the CAIA and governs predictive, not generative AI, systems with the goal of preventing algorithmic discrimination.
- The Act governs high-risk AI systems that make consequential decisions about a human, such as housing, employment, education, healthcare, insurance, and lending. The Act applies to both companies that develop and deploy AI.
- The CAIA is enforced exclusively by the Colorado Attorney General; violations of its requirements are deemed an unfair trade practice under the Colorado Consumer Protection Act, with penalties of up to \$20,000 per violation.
- Developers and deployers have an affirmative defense if they discover and cure violations through their own means or with sought-after feedback from users, so long as they are also otherwise in compliance with the latest Artificial Intelligence Risk Management Framework (AIRMF) published by the National Institute of Standards and Technology (NIST) or another designated framework.
- Colorado's Governor launched the Colorado Artificial Intelligence Impact Task Force, a group of policymakers, industry insiders, and legal experts tasked with identifying where the law works, where it does not, and how to fix it.
- After months of review, the Task Force delivered its report, proposing that the Act require some reconsideration of key provisions. No action has yet been taken to roll back the effective date of February 1, 2026.

Illinois

IL HB-3773: Limit Predictive Analytics Use *(Effective January 1, 2026)*

- This law amends the Illinois Human Rights Act to prohibit the use of AI that results in illegal discrimination within employment recruitment, hiring, promotion, selection for training, or discipline decisions. It also requires notification to employees when using AI during employment decisions. Additional regulations on this amendment are to be issued.

Minnesota

MN HF 4757: Minnesota Consumer Data Privacy Act *(Effective July 31, 2025)*



- This law grants individuals the right to opt out of automated decision-making, the right to question the profiling and the outcome of an automated profiling decision, and to be informed of actions they can take to secure a different decision in the future and the right to review the data used in the profiling.
- For more information about the Minnesota Consumer Data Privacy Act, [read our prior Q&A-style alert](#).

Utah

Utah Artificial Intelligence Policy Act (Effective May 1, 2024)

- The Utah Artificial Intelligence Policy Act (UAIP) establishes liability for using generative artificial intelligence that violates consumer protection laws if not properly disclosed.
- The UAIP requires that "A person who provides the services of a regulated occupation shall prominently disclose when a person is interacting with a generative artificial intelligence in the provision of regulated services."
 - A **regulated occupation** is defined as an occupation regulated by the Utah Department of Commerce that requires a person to obtain a license or state certification. The disclosure requirement for a person in a regulated occupation depends on the form of communication. If it is an oral exchange or conversation, the disclosure must be done verbally at the start of the oral exchange or conversation. If it is a written exchange, the disclosure must be made through electronic messaging before the written exchange.
- Those operating in Utah outside of "regulated occupations" under the UAIP, whose activities are broadly governed under Utah's Division of Consumer Protection, are required to "clearly and conspicuously" disclose the use of generative AI if a consumer requests it.
- The UAIP also creates an Office of Artificial Intelligence Policy, which allows companies introducing AI technologies in Utah to develop regulatory mitigation agreements with the state similar to EU-style consultations and sandboxes. This mitigation can include reduced fines for violations and cure periods before fines are assessed.

State Attorney Generals and Governors are Getting Involved in AI Regulation

- At least three attorney generals in Massachusetts, Oregon, and New Jersey have issued guidance on the use of AI and compliance with existing laws. This guidance highlighted that AI is regulated under existing laws, including consumer protection, data protection, trade protection, and state anti-discrimination laws.
- Additionally, Governors in Texas, New York, and Virginia have banned the use of Deep Seek on state-owned devices and networks, claiming that its AI raises excessive security, privacy, and censorship threats.

State Legislation and Regulations to Watch

Below are some key state AI legislation and actions now being considered:

- So far this year, several states, including Illinois, Hawaii, New York, Nevada, Texas, Virginia, Georgia, Connecticut, and Maryland, have introduced and considered high-risk or comprehensive AI bills.
- Many states, including Massachusetts, New York, Pennsylvania, Virginia, and Hawaii, have also introduced AI transparency bills.
- Several states, including Illinois, New York, Pennsylvania, and Washington, have introduced employment-related AI bills.
- In November 2023, the California Privacy Protection Agency (CPPA) released a set of draft regulations on the use of [artificial intelligence](#) (AI) and automated decision-making technology (ADMT). The proposed rules have been submitted to the CPPA formal rulemaking process to establish consumers' rights to access and opt out of businesses' use of ADMT.



A Federal AI Policy is in the Works

- On January 23, 2025, the Trump Administration rolled back the Biden Administration's Executive Order on AI and issued an Executive Order indicating that by July 2025, the Administration will issue an AI policy to enhance national AI development and security.
- [Subscribe to our Privacy, Cyber, & AI Decoded alerts here](#) to stay tuned for our next installment on further international AI developments.