States Shifting Focus on AI and Automated Decision-Making

Article By:

Alan L. Friel

Julia B. Jacobson

Since January, the federal government has moved away from comprehensive legislation on artificial intelligence (AI) and adopted a more muted approach to federal privacy legislation (as compared to 2024's tabled federal legislation). Meanwhile, state legislatures forge ahead – albeit more cautiously than in preceding years.

As we previously reported, the Colorado AI Act (*COAIA*) is set to go into effect on February 1, 2026. In signing the COAIA into law last year, Colorado Governor Jared Polis (D) issued a letter urging Congress to develop a "cohesive" national approach to AI regulation preempting the growing patchwork of state laws. In the letter, Governor Polis noted his concern that the COAIA's complex regulatory regime may drive technology innovators away from Colorado. Eight months later, the Trump Administration announced its deregulatory approach to AI regulation making federal AI legislation unlikely. At that time, the Trump Administration seemed to consider existing laws – such as Title VI and Title VII of the Civil Rights Act and the Americans with Disabilities Act which prohibit unlawful discrimination – as sufficient to protect against AI harms. Three months later, a March 28th Memorandum issued by the federal Office of Management and Budget directs federal agencies to implement risk management programs designed for "managing risks from the use of AI, especially for safety-impacting and rights impacting AI."

On April 28, two of the COAIA's original sponsors, Senator Robert Rodriguz (D) and Representative Brianna Titone (D) introduced a set of amendments in the form of SB 25-318 (*AIA Amendment*). While the AIA Amendment seems targeted to address the concerns of Governor Polis, with the legislative session ending May 7, the Colorado legislature has only a few days left to act.

If the AIA Amendment passes and is approved by Governor Polis, the COAIA would be modified as follows:

- The definition of "algorithmic discrimination" would be narrowed to mean only use of an AI system that results in violation of federal or Colorado's state or local anti-discrimination laws.
  - The current definition is much broader – prohibiting any condition in which use of an AI system results in "unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived 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 the laws of this state or federal law." (Colo. Rev. Stat. § 6-1-1701(1).)

- Obligations on developers, deployers and vendors that modify high-risk AI systems would be materially lessened.
- An exception for a developer of an AI system offered with "open model weights" (i.e., placed in the public domain along with specified documentation), as long as the developer takes certain technical and administrative steps to prevent the AI system from making, or being a substantial factor in making, consequential decisions.
- The duty of care imposed on a developer or deployer to use reasonable care to protect consumers from any known or foreseeable risks of algorithmic discrimination of a high-risk AI System would be removed.
  - This is a significant change from the focus on procedural risk reduction duties and away from a general duty to avoid harm.
- Developer reporting obligations would be reduced.
- Deployer risk assessment record-keeping obligations would be removed.
- A deployer's notice (transparency) requirements for a consumer who is subject to an adverse consequential decision from use of a high-risk AI system would be combined into a single notice.
- An additional affirmative defense for violations that are "inadvertent", affect fewer than 100,000 consumers and are not the result of negligence on the part of the developer, deployer or other party asserting the defense would be added
- Effective dates would be extended to January 1, 2027, with some obligations pushed back to April 1, 2028, for a business employing fewer than 250 employees, and April 1, 2029, for a business employing fewer than 100 employees.

Even if the AIA Amendment is passed, COAIA will remain the most comprehensive U.S. law regulating commercial AI development and deployment. Nonetheless, the proposed AIA Amendment is one example of how the innovate-not-regulate mindset of the Trump Administration may be starting to filter down to state legislatures.

Another example: in March, Virginia Governor Glenn Yougkin (R) vetoed HB 2094, the High-Risk Artificial Intelligence Developer and Deployer Act, which was based on the COAIA, and a model bill developed by the Multistate AI Policymaker Working Group (*MAP-WG*), a coalition of lawmakers from 45 states. In a [statement](#) explaining his veto, Governo Youking noted that "HB 2094's rigid framework fails to account for the rapidly evolving and fast-moving nature of the AI industry and puts an especially onerous burden on smaller firms and startups that lack large legal compliance departments." Last year California Governor Gavin Newsom (D) [vetoed](#) SB 1047, which would have focused only on large-scale AI models, calling on the legislature to further explore comprehensive legislation and states that "[a] California-only approach may well be warranted – especially absent federal action by Congress."

Meanwhile, on April 23, California Governor Newson warned the California Privacy Protection Agency (*CPPA*) (the administration agency that enforces the California Consumer Privacy Act (*CCPA*)) to reconsider its [draft automated decision-making technology ("ADMT") regulations](#) to leave AI regulation to the legislature to consider. His [letter](#) echoes a letter from the California Legislature, chiding the CPPA for its lack of the authority "to regulate any AI (generative or otherwise) under Proposition 24 or any other body of law." At its May 1st meeting, the CPPA Board considered and approved staff's proposed changes to the ADMT draft regulations, which include deleting the definitions and mentions of "artificial intelligence" and "deep fakes." The revised ADMT draft

regulations also include these revisions (along others):

- Deleting the definition "extensive profiling" (monitoring employees, students or publicly available spaces or use for behavioral advertising) and shifting focusing on use to make a significant decision about consumers. Reducing regulation of ADMT training. However, risk assessments would still be required for profiling based on systemic observation and training of ADMT to make significant decisions or to verify identity or for biological or physical profiling.
- Streamlining the definition of ADMT to "mean any technology that processes personal information and uses computation to replace … or substantially replace human decision-making [which] means a business uses the technology output to make a decision without human involvement."
- Streamlining the definition significant decisions to remove decisions regarding "access to," and limited to "provision or denial of" the following more narrow types of goods and services: "financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services," and clarifying that use for advertising is not a significant decision.
- Deleting the obligation to conduct specific risk of error and discrimination evaluations for physical or biological identification or profiling, but the general risk assessment obligations were largely kept.
- Pre-use notice obligations were streamlined.
- Opt-out rights were limited to uses to make a significant decision.
- Giving businesses until January 1, 2027, to comply with the ADMT regulations.

(A more detailed analysis of the CCPA's rule making, including regulation unrelated to ADMT, will be posted soon.)

MAP-WG inspired bills also are under consideration by several other states, including California. Comprehensive AI legislation proposed in Texas, known as the Texas Responsible AI Governance Act, was recently substantially revised (HB 149) to shift the focus from commercial to government implementation of AI systems. (The Texas legislature has until June 2 to consider the reworked bill.) Other states have more narrowly tailored laws focused on Generative AI – such as the Utah Artificial Intelligence Policy Act which requires any business or individual that "uses, prompts, or otherwise causes [GenAI] to interact with a person" to "clearly and conspicuously disclose" that the person is interacting with GenAI (not a human) "if asked or prompted by the person" and, for persons in "regulated occupations" (generally, need a state license or certification), disclosure must "prominently" disclose that a consumer is interacting with generative AI in the provision of the regulated services.

What happens next in the state legislatures and how Congress may react is yet to be seen. Privacy World will keep you updated.