The Computer & Internet Lawyer

Volume 43 ▲ Number 9 ▲ October 2026

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Connecticut Enacts AI Framework While Colorado Scales Back Landmark AI Law

By Duane C. Pozza, Kathleen E. Scott and Lauren N. Lerman

States continue to play a leading role in shaping artificial intelligence (AI) regulation in the absence of a comprehensive federal framework. Two recent developments demonstrate how state approaches to AI regulation are evolving in different ways.

First, on May 14, 2026, Colorado Senate Bill 26-189[1] (Revised Colorado AI Act) was signed into law, repealing and reenacting the 2024 Colorado Artificial Intelligence Act with amendments.

Second, on May 29, 2026, the Connecticut governor signed into law the Connecticut Artificial Intelligence Responsibility and Transparency Act[2] (Connecticut AI Act), a multi-part law that imposes targeted requirements across several high-profile AI use cases, including chatbots, synthetic media, and automated decision-making.

This article provides a high-level overview of (1) the Revised Colorado AI Act, highlighting how the state has scaled back its earlier risk-based framework in favor of a more limited transparency-focused regime, and (2) the Connecticut AI Act and its targeted, use-case-specific approach to AI regulation.

The authors, attorneys with Wiley Rein LLP, may be contacted at dpozza@wiley.law, kscott@wiley.law and llerman@wiley.law, respectively.

REVISED COLORADO AI ACT

The Revised Colorado AI Act, which will go into effect on January 1, 2027, significantly pares down requirements that would have been applicable under the 2024 Colorado Artificial Intelligence Act, which never went into effect. The Revised Colorado AI Act favors transparency and disclosure obligations over prescriptive governance requirements. In particular, the 2026 law makes several notable changes to the 2024 law, as described below.

Scope

The Revised Colorado AI Act applies to developers and deployers of automated decision-making technologies (ADMT) that materially influence covered consequential decisions about Colorado consumers. ADMT is defined as "a technology that processes personal data and uses computation to generate output, including predictions, recommendations, classifications, rankings, scores, or other information that

is used to make, guide, or assist a decision, judgment, or determination concerning an individual." The law also defines "materially influence" and "covered consequential decision" to encompass decisions made by, or with significant input from, an ADMT that relate to consumer access, eligibility, or compensation in a variety of domains, such as education, employment, and health care.

Revised Obligations

The 2026 version of the law removes several of the original 2024 law's most burdensome obligations, including mandatory risk management programs, annual impact assessments, and broad "duty of care" obligations to prevent algorithmic discrimination. Instead, the Revised Colorado AI Act requires:

- Notice by deployers to individuals when AI is used in consequential decisions;
- Disclosures by deployers regarding how automated tools affect outcomes;
- Opportunities for individuals to seek human review or corrections from a deployer;
- Documentation and information-sharing between developers and deployers;
- Recordkeeping by deployers of ADMT outputs covered by the law and by developers of ADMT changelogs and material updates; and
- Mechanisms and a policy by deployers for providing consumers recourse when impacted by an adverse outcome.

The Colorado Attorney General is tasked with adopting clarifying rules by January 1, 2027, and that office will be the government agency responsible for enforcing the Revised Colorado AI Act. The law requires the Attorney General to provide a 60-day notice and cure period before bringing an enforcement action, except for recurring violations.

CONNECTICUT AI ACT

Connecticut's new AI law combines several separate AI proposals into one law, creating more of a modular approach with targeted obligations across discrete AI use cases rather than a single, unified framework. Connecticut's law takes effect between October 2026 and January 2028, depending on the provision. Several notable provisions of the law are discussed below.

AI Subscriptions

"Subscription-based providers," defined as persons doing business in Connecticut to provide AI technology to consumers pursuant to a subscription, must (1) provide written notice about the subscription and the nature of the AI offering, and (2) obtain written consumer consent, before providing the subscription and collecting a fee or other compensation for the AI technology subscription.

Whistleblower Protection for Employees of Frontier Models

Frontier AI model developers are prohibited from firing or otherwise penalizing employees for reporting that the developer "engaged in any activity that poses a specific and substantial danger to the public health or safety due to a catastrophic risk." Frontier developers must also establish an internal process for reporting such health and safety risks and provide employees with annual notice of their rights and responsibilities under this section of the law.

AI Companions

Providers of AI companions must include a protocol that detects potential user expressions of self-harm or physical violence and refers users to helpful resources if such expressions are detected. Operators of AI companions must also provide notice to consumers that they are interacting with an AI system and not a human. AI companions may not be provided to consumers under the age of 18 (if the operator knows, or has reason to believe, that the user is younger than 18) unless the operator has implemented safeguards that meet or exceed industry standards to prevent harmful or manipulative engagement with the companion. As a few examples, the law seeks to prevent AI companions from encouraging minors to harm themselves or others, providing mental health advice or discouraging mental health advice, or engaging in romantic or sexual relationships with the user.

The law defines AI companion to be any form of AI "with a natural language interface that (i) provides adaptive, human-like responses to user inputs, including, but not limited to, by exhibiting anthropomorphic features, and (ii) is able to sustain a relationship across multiple interactions" with key exceptions for:

(1) chatbots used exclusively for business purposes or that are part of a video game;

(2) certain stand-alone consumer electronic devices;

(3) narrowly tailored educational tools;

(4) certain AI systems solely used to provide health care-related support; and

(5) narrow, task-specific tools that provide outputs relating to a discrete topic or function.

Employment ADMT

Developers of automated employment-related decision technology that advertise, market, or sell ADMT for use in materially influencing an employment-related decision must provide deployers of such ADMT with all information the deployers need to perform their duties or otherwise contractually assume those duties. Deployers of employment-related ADMT must (1) disclose to employees or applicants that they are interacting with such technology, and (2) provide employees or applicants with written notice, before generating an output for the purpose of making an employment-related decision, that ADMT is being used, the purpose of the ADMT and the related employment decision, the personal data being used, and relevant contact information. The law also amends Connecticut's Fair Employment Practices Act to state explicitly that use of ADMT in employment-related decisions is not a defense to a complaint alleging a discriminatory employment practice.

The law defines "automated employment-related decision technology" to be "any technology that processes personal data and uses computation to generate any output, including, but not limited to, any prediction, recommendation, classification, ranking, score or other information, that is a substantial factor used to make or materially influence an employment-related decision," with key exceptions for:

(1) software or technology that does not make or materially influence an employment-related decision (examples include word processing, web hosting, networking, data storage, anti-virus, spam and robocall filtering, and spellchecking);

(2) any system or service that is used in a manner that is incidental to making an employment-related decision; or

(3) information that is purely descriptive, diagnostic, or statistical in nature and not relied upon to make or materially influence an employment-related decision.

Synthetic Media

A "covered provider," defined as "any person who creates, codes, or otherwise produces a generative artificial intelligence system that (i) has more than one million users per month, and (ii) is publicly accessible to consumers for personal use," must include provenance data in any audio, image, video, or other content that is created or materially altered by generative AI, as a mechanism for disclosing that the content was synthetically generated. Such provenance data must use technically reasonable methods and standards, without disclosure of personally identifiable information or trade secrets. The section also exempts business-to-business sales and use of generative AI systems and products that exclusively provide video game or interactive experiences.

These laws follow regulatory efforts in California, New York, and other states to address AI.

Social Media

A "covered platform," defined as a website, online service, online application, mobile application, or social media platform that "recommends, selects or prioritizes for display, either concurrently or sequentially, media items generated or shared on a platform by users of such platform," must obtain consent before providing its algorithmic services to minors. The covered platform must use commercially reasonable and technically feasible methods to determine that a user is not a minor. Additionally, the covered platform must display to minors a warning in black and white that says, "The Surgeon General has warned that while social media may have benefits for some young users, social media is associated with significant mental health harms and has not been proven safe for young users."

AI Regulatory Sandbox and Pilot Programs

In addition to establishing specific obligations as described above, the law establishes an AI regulatory sandbox program to allow an applicant to "temporarily test an innovative product or service on a limited basis under reduced licensure, regulatory and other legal requirements than may otherwise be required under the laws of the state," and a pilot program for independent third-party entities to evaluate the use of independent verification programs that assess the "adherence of artificial intelligence models to standards reflecting best practices for the prevention of

personal injury, property damage, data privacy harms and other harms."

New Working Groups and Advisory Boards

The law further creates several working groups and advisory boards and directs state agencies and legislative leadership to undertake research and reporting on the use and development of AI for state government purposes, while also recommending future legislation and advancing AI education and innovation.

CONCLUSION

These laws follow regulatory efforts in California, New York, and other states to address AI. As states continue adopting materially different approaches to AI regulation, creating a fragmented compliance landscape, companies should take proactive steps to strengthen AI governance and continuously monitor emerging requirements to adapt their compliance strategies accordingly.

Notes

1. https://leg.colorado.gov/bill_files/116489/download.
2. https://www.cga.ct.gov/2026/ACT/PA/PDF/2026PA-00015-R00SB-00005-PA.PDF.

Copyright © 2026 CCH Incorporated. All Rights Reserved.
Reprinted from *The Computer & Internet Lawyer*, October 2026, Volume 43, Number 9, pages 12–14 with permission from Wolters Kluwer, New York, NY, 1-800-638-8437, www.WoltersKluwerLR.com

