POLSINELLI

Publications

February 25, 2025 • Updates

Some States Step Up Early to Regulate AI Risk Management

Key Takeaways

- A global AI arms race may mean U.S. states are best positioned to regulate AI's risks.
- Colorado and Utah have enacted legislation for how AI is to be used with consumers.
- Other states are emphasizing existing laws they say "have roles to play" in regulating AI.

In the span of one month, an executive order issued in 2023 focusing on artificial intelligence (AI) safety and security was repealed and replaced by an executive order focusing on the U.S. being the global leader in AI innovation, while in the EU a liability directive developed in 2022 was abandoned in favor of a bolder, simpler and faster 2025 Commission work program, with an "ambition to boost competitiveness."

A 'move fast and break things' approach to an emerging technology arms race often has drawbacks. For example, the recent rise of DeepSeek provided a glimpse into what was previously unimaginable: an open-source large language model useful for a wide range of purposes, that's fast, cheap and scalable. But within days it was hacked, sued and discredited.

While nations battle for AI supremacy by "removing barriers" and loosening regulations, in the U.S. last year, 45 states introduced AI bills, and 31 states adopted resolutions or enacted legislation. Overall, hundreds of bills in 23 different AI-related categories have been considered. Two states standout, Colorado and Utah, for their focus on consumer protection.

Colorado's AI Act

The Colorado Artificial Intelligence Act (CAIA), which goes into effect on February 1, 2026, applies to developers and deployers of high-risk AI systems. A developer is an entity or individual that develops or intentionally and substantially modifies a high-risk AI system, and a deployer is an individual or entity that deploys a high-risk AI system. A high-risk AI system is one used as a substantial factor in making a consequential decision.

A consequential decision means a decision that has a material legal or similarly significant

Related People

- Romaine C. Marshall
- Taryn A. Elliott
- Spencer R. Wood
- Jennifer Bauer

Related Capabilities

- Artificial Intelligence & Machine Learning
- US State Privacy Laws
- Technology Transactions
- Privacy & Cybersecurity

effect on the provision or denial to any consumer of, or the terms of, education, employment, a financial or lending service government service, healthcare service, housing, insurance or legal service.

These definitions of the CAIA can seem abstract when not applied to use cases. But a standout feature of the CAIA are its robust mitigation techniques which include a safe harbor if the National Institute of Standards and Technology's AI Risk Management (NIST AI RMF) is considered when devising a Risk Management Policy and Program, which is required.

The NIST AI RMF provides voluntary guidance to individuals and companies on how to best manage AI risks throughout an AI system's lifecycle, often referred to as the implementation of Trustworthy AI, which includes such characteristics as reliability, safety, security, resilience, accountability, transparency and fairness.[1]

The CAIA requires that deployers and developers meet certain criteria to ensure they understand what is required to protect consumers from known or foreseeable risks. In addition to a risk management policy and program, covered entities must complete impact assessments at least annually and in some instances within 90 days of a change to an AI system.

An impact assessment under CAIA requires substantial documentation. For instance, the assessment must include such things as a statement, an analysis, a description and overview of the data used, metrics, a description of transparency measures, and post-deployment monitoring and user safeguards.

Utah's AI Policy Act

Utah is also an early adopter of AI legislation. In fact, the Utah Artificial Intelligence Policy Act (UAIP) has been in effect since May 2024. Among other things, the UAIP seeks to simultaneously increase consumer protections and encourage responsible AI innovation by:

- Mandating transparency through consumer disclosure requirements;[2]
- Clarifying liability for AI business operations, including key terms and legal defenses;
- Enabling innovation through a regulatory sandbox for responsible AI development, regulatory mitigation agreements (RMAs) and policy and rulemaking by a newly created Office of Artificial Intelligence Policy (OAIP).

The statutory inclusion of RMAs is a unique example of how Utah aspires to balance AI's potential risks and rewards. The UAIP defines RMAs as an agreement between a participant, OAIP and relevant state agencies and defines regulatory mitigation as restitution to users, cure periods, civil fines if any and other terms that are tailored to the AI technology seeking mitigation.

While not quite a safe harbor from all liability, RMAs provide AI developers, deployers and users with an opportunity to test for unintended consequences in a somewhat controlled environment. In December, the OAIP announced that it had executed its first RMA with ElizaChat, an app schools can offer teens for their mental health.

The 12-page RMA with ElizaChat is notable for its multiple references to cybersecurity – an area the UAIP intends to eventually establish standards for – and schedules. Included in Schedule A under the subheading "Mitigation Offered" are detailed requirements the ElizaChat app must meet, including a Testing Plan and notification obligations should

certain incidents occur.[3]

As to AI liability, the UAIP specifies and clarifies that businesses cannot blame AI for any statutory offenses. The fact that AI "made the violative statement, undertook the violative act, or was used in furtherance of the violation" is irrelevant and cannot be used as a legal defense.[4] The UAIP also contemplates the creation of AI cybersecurity standards through the OAIP.

The UAIP also establishes a Learning Lab through which businesses can partner with the OAIP to responsibly develop and test AI solutions. In this way, the UAIP sets the stage for a new era of AI regulation by being the first state law to embed cross-functional learning opportunities for future rules and regulation.

Other States Are Ready to Regulate

On the day this article was published, Virginia announced it passed an AI bill. It is similar to the Colorado and Utah AI Acts with references to AI disclosures and liability standards and the NIST AI RMF. Connecticut also reintroduced "An Act Concerning AI" and New Mexico introduced an anti-algorithmic discrimination bill.

Not to be outdone, in the last few months several states' attorneys general (AGs) have issued guidance on how they intend to protect consumers and what they expect from organizations that develop, sell and use AI, none more forcefully as AG Rosenblum of Oregon: "If you think the emerging world of AI is completely unregulated under the laws of Oregon, think again!"

AG Rosenblum discusses how Oregon's Unlawful Trade Practices Act, Consumer Privacy Act and Equality Act affect implementation of AI, even providing seven examples under the UTPA. AG Bonta of California followed suit a week later in a seven-page advisory, citing similar laws and providing nine examples of violations of its unfair competition law.

How to Prepare

To be sure, it's still early. But states' regulation of AI and their inclusion of voluntary guidance frameworks such as the NIST AI RMF or RMAs provide, at a minimum, iterative starting points for the types of industry standards that will emerge as legal obligations. Therefore, organizations should consider whether their policies, procedures and plans will enable them to leverage them.

[1] For further background on the NIST AI RMF see here https://www.polsinelli.com/romaine-c-marshall/publications/artificial-intelligence-has-a-nist-framework-for-cybersecurity-risk (May 2023) and here https://www.polsinelli.com/romaine-c-marshall/publications/nist-releases-risk-profile-for-generative-ai (May 2024).

[2] Yesterday, the UAIP's original sponsors proposed an amendment to the required disclosures section, narrowing its application to "high-risk artificial interactions" which refers to interactions with generative AI involving health, financial, medial, and mental health data. If passed, this limitation to the required disclosures will go into effect in June of this year. https://le.utah.gov/~2025/bills/static/SB0226.html. If adopted, this limitation would go some way to lessening the burden of compliance for small and medium businesses.

[3] *Id*. at 8.

[4] Utah Code. Ann. section 13-2-12 (2).