CLIENT ALERTS & INSIGHTS

Colorado Jumps to Head of the Line, Enacts First Comprehensive State AI Consumer Protection Law

MAY 31, 2024

Authors: Megan C. Parker, Kristopher J. Chandler

Colorado's comprehensive artificial intelligence legislation signals that future AI regulation is trending toward a state-by-state approach, like data privacy before it, unless federal legislation is enacted.

On May 17, 2024, Colorado Gov. Jared Polis signed into law SB 24-205, Consumer Protections for Interactions with Artificial Intelligence (the "**Colorado AI Act**"), making Colorado the first U.S. state to enact comprehensive legislation regarding the use and development of artificial intelligence ("**AI**").

The Colorado AI Act, which goes into effect Feb. 1, 2026, is designed to require deployers and developers of high-risk AI systems use reasonable care in preventing algorithmic discrimination.

Scope

The Colorado AI Act only applies to developers and deployers using high-risk AI systems that are doing business in Colorado, regardless of the number of consumers impacted. The requirements and obligations related to prevention of algorithmic discrimination vary depending on whether an entity constitutes a deployer or developer.

A deployer is defined as "a person doing business in [Colorado] that deploys a high-risk [AI] system" whereas a developer is defined as "a person doing business in [Colorado] that develops or intentionally and substantially modifies an [AI] system."

Importantly, the Colorado AI Act defines a high-risk AI system as "any [AI] system that, when deployed, makes, or is a substantial factor in making, a consequential decision." A consequential decision means any decision that "has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of:" (1) education, (2) employment, (3) credit, (4) government services, (5) healthcare, (6) housing, (7) insurance or (8) legal services.

AI systems intended to perform a narrow procedural task or detect decision making patterns or deviations without replacing or influencing a previously completed human assessment are explicitly excluded from being high-risk AI systems. The Colorado AI Act also excludes certain technologies, like cybersecurity software and spam filtering, when they are not a substantial factor in consequential decisions.

Lastly, algorithmic discrimination includes "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 protected classifications, such as age, disability, race, religion or sex.

Any discrimination, however, resulting from use of a high-risk system for the sole purposes of (1) self-testing AI systems to identify and rectify incidents or risks of discrimination or (2) expanding an

applicant, customer or participant pool to increase diversity, do not constitute algorithmic discrimination the Colorado AI Act aims to prevent.

Requirements and Obligations

The Colorado AI Act imposes several documentation, disclosure and compliance obligations on developers and deployers intended to identify and prevent algorithmic discrimination.

First, both developers and deployers are requested to exercise reasonable care in preventing algorithmic discrimination. Although no definition is given for reasonable care, the Colorado AI Act provides rebuttable presumptions to show the exercise of reasonable care.

Developer Rebuttable Presumptions

A developer of a high-risk AI system will be deemed to have exercised reasonable care to avoid algorithmic discrimination if the developer:

- Provides deployers with information about the system, including its purpose, intended benefits / uses, operation, potential risks, and any known or foreseeable algorithmic discrimination.
    - Additionally, the developer must provide information on how the system was trained and evaluated for performance, including any resulting evidence of algorithmic discrimination.
- Provides deployers with all documentation necessary to conduct an impact assessment.
- Makes publicly available a summarization of the types of high-risk AI systems developed or intentionally and substantially modified by the developer.
- Provides deployers with information on how the developer mitigates any reasonable or foreseeable risk of algorithmic discrimination in developing or later modifying the AI system.
- Discloses to the Colorado State Attorney General and deployers any known or reasonably foreseeable risks of algorithmic discrimination within 90 days of being informed or learning of such risks.

Deployer Rebuttable Presumptions

The Colorado AI Act creates a two-tiered rebuttable presumption that deployers of a high-risk AI system exercised reasonable care to avoid algorithmic discrimination.

For all deployers, the rebuttable presumption applies if the deployer:

- Reviews the deployment of each high-risk AI system at least annually for evidence of algorithmic discrimination.

- Provides consumers information about consequential decisions concerning the consumer made by high-risk AI systems and giving the consumer an opportunity to correct any incorrect personal data used in making such consequential decisions.
    - Additionally, deployers must provide consumers with an opportunity to appeal an adverse consequential decision made by a high-risk AI system through human review, where technically feasible.

- Discloses to the Colorado State Attorney General, within 90 days of discovery, when a high-risk AI system has or is reasonably likely to have caused algorithmic discrimination.

Next, for deployers who, at all times, a high-risk AI system is deployed: (1) have 50 or more full-time employees, (2) does not use the deployer's own data to train the high-risk AI system, and (3) uses a high-risk AI system only for the intended uses disclosed by the developer, the rebuttable presumption applies if the deployer:

- Implements risk management policies and programs for high-risk AI systems.
- Conducts impact assessments for each high-risk AI system deployed.
- Makes publicly available a summary of the types of high-risk AI systems deployed, including how the deployer manages any known or foreseeable risk of algorithmic discrimination.
- Makes publicly available information about the nature, source and extent of information collected and used by the deployer in a high-risk AI system.

Disclosure of AI Interaction

Lastly, like other state legislation on AI, the Colorado AI Act requires any developer or deployer who makes available *any* AI system that is intended to interact with consumers to disclose to consumers that they are interacting with an AI system and not a live person.

Enforcement and Penalties

The Colorado State Attorney General has the exclusive authority to enforce violations, with a penalty of up to $20,000 per violation.

The Attorney General also has the authority to promulgate rules as necessary to implement and enforce the Colorado AI Act, including requirements for documentation, disclosures, risk management policies, impact assessments, rebuttable presumptions and affirmative defenses.

Meanwhile, developers, deployers or other parties can assert an affirmative defense if they: (1) discover and cure a violation, and (2) comply with the latest version of the Artificial Intelligence Risk Management Framework published by the National Institute of Standards and Technology, or any other framework designated by the Colorado State Attorney General.

Conclusion and Takeaways

While the Colorado AI Act joins the list of recent legislative and regulatory efforts to regulate the development and use of AI, including President Biden's Executive Order on AI, the legislation sets significant precedent for a comprehensive roadmap on regulating AI at the state and federal levels.

Set to take effect Feb. 1, 2026, developers and deployers of AI systems will have less than two years to ensure compliance with the Colorado AI Act's requirements. Given how technically complex AI models are, companies that develop or deploy high-risk AI systems should take a compliance-by-design approach in building AI models.

Continue to follow Benesch's AI Commission as we address the evolving regulatory landscape of AI, impacts of new regulations and steps toward compliance. Stay tuned!

With thanks to Benesch summer associate, Andrew Klemm (J.D. '25 candidate, Case Western Reserve University School of Law), who assisted with preparing this article.