wiley

ALERT

Colorado Enacts Landmark AI Legislation

May 20, 2024

On May 17, 2024, Colorado Governor Jared Polis signed into law SB24-205 — Consumer Protections for Artificial Intelligence (Colorado AI Act) — making Colorado as the first state to adopt broad artificial intelligence (AI) legislation. While other states have enacted AI-specific legislation, including a new law in Utah that establishes disclosure requirements for certain uses of generative AI, the landmark Colorado AI Act more broadly establishes requirements for developers and deployers of "high-risk artificial intelligence systems," as well as disclosure requirements for AI systems that are intended to interact with consumers.

The new law is notable not just as a "first" in AI regulation in the United States, but also in its level of complexity: it establishes a range of detailed obligations for AI developers and deployers. The Colorado AI Act also gives the state's Attorney General (AG) plenary rulemaking authority, pointing to even more detailed regulations to come, as we have seen with the Colorado Privacy Act rules.

The new law will go into effect on February 1, 2026 — which will give companies that develop and deploy AI some time to understand and operationalize this groundbreaking new framework, which is complex and includes nuanced thresholds and exceptions. Below we provide a high-level breakdown of the Colorado AI Act to help companies understand the general framework.

Much of the Colorado AI Act Focuses on "High-Risk Artificial Intelligence Systems"

The new law establishes obligations for developers and deployers of "high-risk artificial intelligence systems." A high-risk AI system is defined to include "any [AI] system that, when deployed, makes or is a substantial factor in making, a consequential decision." The law

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Practice Areas

Artificial Intelligence (AI)
Privacy, Cyber & Data Governance
State Privacy Laws
State Regulation

further defines "consequential decision" to be one that has a "material legal or similarly significant effect on the provision or denial, to any consumer of, or the cost or terms of" a defined category of opportunities and services, to include:

- Education enrollment or an education opportunity;
- Employment or an employment opportunity;
- A financial or lending service;
- An essential government service;
- Health-care services;
- Housing;
- Insurance; or
- A legal service.

Obligations of Developers of High-Risk AI Systems

The Colorado AI Act places a duty of reasonable care on developers of high-risk AI systems to protect consumers from known or reasonably foreseeable risks of "algorithmic discrimination" arising from high-risk AI systems. "Algorithmic discrimination" is defined as any "condition in which the use of an artificial intelligence system results in an 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 [Colorado] or federal law."

The law creates a rebuttable presumption of reasonableness for the developers if they execute the following requirements:

1. **Disclosures and Documentation for Deployers.** Developers of high-risk AI must make available to deployers or other developers: a general statement describing reasonably foreseeable harmful uses of its high-risk AI system; documentation detailing the data used to train the system, limitations of the system, purposes and intended use for the system, and how the system was tested for algorithmic discrimination and any subsequent remedies implemented to mitigate any discrimination risk revealed during the testing; and documentation needed for deployers to conduct impact assessments. Of note, the new law contemplates that the AG may require that a developer disclose this documentation to the AG, as well.
2. **Public Disclosures.** A developer of high-risk AI systems must include on its website a statement describing the types of high-risk AI systems the developer currently makes available to deployers and how the developer mitigates reasonably foreseeable algorithmic discrimination that stems from its AI system.
3. **Discrimination Risk Disclosures to the AG and Deployers.** A developer of high-risk AI systems must disclose to the AG (and to all known deployers or other developers of its AI systems) known or

reasonably foreseeable discrimination risks arising from intended uses of its high-risk AI systems no later than 90 days after the developer is made aware of such risks either through its own ongoing testing or through a credible report indicating such a risk exists.

Obligations of Deployers of High-Risk AI Systems

Deployers of high-risk AI systems are also subject to a duty of reasonable care to protect consumers from known or reasonably foreseeable risk of algorithmic discrimination arising from high-risk AI systems. As is the case with developers, deployers can also rely on a rebuttable presumption of reasonableness where the deployer does the following:

1. Implements a **risk management policy and program**. The new law provides details and parameters around what a reasonable policy and program should be, and points deployers to the NIST AI Risk Management Framework (among other guidance) for consideration.
2. Completes **impact assessments** of high-risk AI systems.
3. Provides **consumer notice, disclosures, and rights, as applicable,** with respect to consequential decisions. Specifically, before a consequential decision is made, deployers must provide consumers with notice that the deployer has deployed a high-risk AI system to make, or be a substantial factor in making, consequential decisions, statements that explain the nature of the decision and a description of the system, and information (if applicable) about the consumer's right to opt-out of profiling under the Colorado Privacy Act. If the consequential decision is adverse to a consumer, the deployer must provide the consumer a statement disclosing the reasons for the decision and the data used to make the decision, an opportunity to correct incorrect personal data, and an opportunity to appeal that will include human review (if technically feasible).
4. Provides a **website statement** describing the types of high-risk AI systems the deployer currently uses, how the deployer mitigates reasonably foreseeable algorithmic discrimination that stems from its AI system, and the nature and extent of information collected and used by the deployer.
5. **Discloses to the AG** a discovery that the high-risk AI has caused algorithmic discrimination, within 90 days of the discovery.

Disclosure Requirements for Developers and Deployers of Interactive AI

While most the new law's provisions focus on high-risk AI systems, it also establishes a broader consumer notice requirement for any AI system that "is intended to interact with consumers," except for instances where "it would be obvious to a reasonable person that the person is interacting with an AI system."

***

The Colorado AI Act is a significant step in the regulation of AI, including both AI development and use of AI tools by businesses in Colorado. As with consumer privacy laws, it raises the possibility of a patchwork state-by-state regulatory approach that poses challenges for implementation. Even standing alone, the law and potential AG regulations will require close attention by companies using AI — and considering using AI — for a

wide range of purposes.

Wiley's Artificial Intelligence Practice counsels clients on AI compliance, risk management, and regulatory and policy approaches, and we engage with key government stakeholders in this quickly moving area. Please reach out to a member of our team with any questions.