

Colorado Passes First-in-Nation Artificial Intelligence Act



CONTRIBUTORS



Maneesha Mithal



Christopher N. Olsen



Stacy Okoro

ALERTS

May 21, 2024

On May 17, 2024, Governor Jared Polis signed the [Colorado Artificial Intelligence Act \(SB 24-205\) \(CAIA\)](#), regulating the development, deployment, and use of artificial intelligence (AI) systems. Colorado is the first state to enact comprehensive AI legislation. The law becomes effective February 1, 2026.

Summary

- CAIA applies generally to developers and deployers of “high risk AI systems” (HRAIS), which are defined as AI systems that make, or are a substantial factor in making, a “consequential decision.”
- CAIA imposes a duty of reasonable care on developers and deployers to avoid “algorithmic discrimination” in high-risk AI systems. If a developer or deployer complies with the disclosure, risk assessment, and governance requirements in the statute, there will be a rebuttable presumption that the developer or deployer has used reasonable care to avoid algorithmic discrimination.
- Colorado's attorney general (AG) will be able to enforce the law as an unfair or deceptive trade practice, with a penalty of up to \$20,000 per violation. CAIA does not include a private right of action.

Key Takeaways

- The law is largely limited to AI systems that involve automated decision making about consumers. Most requirements under CAIA do not apply to general purpose AI systems, which are not considered high-risk AI systems. The only requirement for these types of non-high-risk AI systems is a requirement to transparently disclose the use of AI.
- CAIA provides an affirmative defense to enforcement for companies that have 1) cured violations as a result of external feedback or red teaming; and 2) complied with the latest version of the NIST AI risk management framework or an equivalent framework. Establishing robust AI governance programs will be crucial to compliance and can help protect against enforcement if something goes wrong.
- CAIA has similarities with the EU AI Act, which is expected to be adopted in the coming weeks. Both acts implement a risk-based approach and impose similar duties of transparency and data governance. However, the EU AI Act applies more broadly and includes obligations not found in the CAIA. In addition, several other states are considering AI legislation, which may add challenges as companies seek to develop a global compliance framework.

Detailed Analysis

Scope

The CAIA applies to developers and deployers of HRAIS. Developers are defined as any person¹ doing business in Colorado that develops or intentionally and substantially modifies an AI system. Deployers are defined as any person doing business in Colorado that deploys a HRAIS. The law exempts covered entities subject to the Health Insurance Portability and Accountability Act, certain financial institutions, and government contractors.

A high-risk AI system (HRAIS) is “any artificial intelligence system that, when deployed, makes, or is a substantial factor in making a consequential decision.” A “consequential decision” is “a 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: (a) education enrollment or an education opportunity; (b) employment or an employment opportunity; (c) a financial or lending service; (d) an essential government service; (e) health-care services; (f) housing; (g) insurance; or (h) a legal service.”

The term HRAIS excludes, among other things, anti-fraud technology that does not use facial recognition technology, anti-malware, cybersecurity, data storage, AI-enabled video games, chat features, and web caching, so long as they do not make, or are not a substantial factor in making, a consequential decision. Significantly, the term excludes “technology that communicates with consumers in natural language for the purpose of providing users with information, making referrals or recommendations, and answering questions and is subject to an accepted use policy that prohibits generating content that is discriminatory or harmful.” This text would appear to exclude popular generative AI products currently used by consumers.

Developer Duties

The CAIA broadly requires developers of HRAIS to “use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended and contracted uses of the high-risk artificial intelligence system.” “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 this state or federal law.”

Developers can establish a rebuttable presumption that they complied with the “reasonable care” standard if they demonstrate their compliance with the following requirements:

Disclosures to other developers and deployers: Developers must make available to deployers or other developers of HRAIS:

- A general statement describing the reasonably foreseeable uses and known harmful or inappropriate uses of the HRAIS;
- High-level summaries of the training data for the HRAIS, known or reasonably foreseeable limitations of the HRAIS, purpose of the HRAIS, intended benefits and uses of the HRAIS, and any other information necessary to allow the deployer to comply with its own disclosure requirements;
- Documentation about i) how the HRAIS was evaluated for performance and mitigation for algorithmic discrimination, ii) the data governance measures used to cover the training datasets, iii) the intended outputs of the HRAIS; iv) measures to mitigate risks; and v) how the HRAIS should be used, not used, or monitored by an individual when it is being used to make a consequential decision;

Public disclosure: Developers also must disclose on their website or in a public use case inventory, a statement summarizing 1) the types of HRAIS that the developer has developed or intentionally and substantially modified and currently makes available to a deployer or other developer; and 2) how the developer manages known or reasonably foreseeable risks of development or intentionally and substantially modification of HRAIS.

Reporting to the AG: If a developer learns that its HRAIS has been deployed and has caused or is reasonably likely to have caused algorithmic discrimination or if the developer receives a credible report from a deployer that its HRAIS has caused algorithmic discrimination, it must disclose that to the AG and all known deployers or other developers within ninety days of discovery. The AG may also request the documentation described above, which the developer of the HRAIS must provide within 90 days.

Deployer Duties

Similarly, the CAIA requires deployers of HRAIS to “use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination.” Deployers can establish a rebuttable presumption that they meet this standard if they can demonstrate their compliance with the following requirements:

- **Risk management:** Developing a risk management policy and governance program. Guidance and standards for this program must follow the most up-to-date Artificial Intelligence Risk Management Framework released by NIST² or any other nationally (or internationally) recognized risk management framework, or another risk management framework the AG designates as acceptable;
- **Impact assessment:** Completing an impact assessment for the HRAIS, annually and within 90 days of any intentional and substantial modification to the HRAIS;
- **General notification about the use of an HRAIS system:** Notifying consumers if the deployer uses a HRAIS to make, or be a substantial factor in making, a consequential decision concerning a consumer. Deployers must provide the consumer with a statement disclosing information such as the purpose of the system and nature of the consequential decision and, if applicable, information regarding the right to opt out of profiling under the Colorado Privacy Act;
- **Adverse action notices:** If the HRAIS is used to make a consequential and adverse decision to the consumer, the deployer must provide the consumer with i) a statement disclosing the reasons for the consequential decisions, ii) an opportunity to correct any incorrect personal information that was processed the HRAIS in making a decision, and iii) an opportunity to appeal the adverse decision;
- **Website disclosures:** Making available on their websites a statement summarizing information such as the types of HRAIS that are currently deployed by the deployer and how they manage known or reasonably foreseeable risks of algorithmic discrimination.
- **Reporting to AG:** If a deployer discovers that its HRAIS has been deployed and has caused algorithmic discrimination, it must disclose that to the AG within 90 days of discovery. The AG is also entitled to ask for the risk management policy and impact assessments described above, which the deployer must provide within 90 days.

Deployer businesses do not need to comply with the risk management, impact assessment, and website disclosure requirements, if they 1) employ fewer than 50 employees and do not use their own data to train the HRAIS; and 2) make certain disclosures to consumers.

General Transparency Requirements

Separate from the disclosure requirements related to the HRAIS, CAIA also requires consumer-facing developers and deployers to provide notice to consumers when they are interacting with an AI system, unless it would be obvious to a reasonable person.

Enforcement and Civil Penalties

CAIA does not provide a private right of action for consumers and will be exclusively enforced by the Colorado AG or district attorneys. For the purposes of enforcement, violations of the CAIA will be treated as unfair or deceptive trade practices in accordance with the Colorado Consumer Protection Act.

If the AG brings an action against a developer or deployer, these entities have an affirmative defense if 1) they discover and cure the violation in accordance with public feedback, red teaming, or an internal review process and 2) they have implemented and maintained a program that is in compliance with NIST’s Artificial Intelligence Risk Management Framework, another nationally or internationally recognized risk management framework for AI, or a risk management framework designated by the AG.

The Colorado AG is also allowed, but not required, to engage in rulemaking regarding the documentation and requirements for developers, notices, and disclosures related to AI, the requirements for establishing the risk management policy and program, the content and requirements for impact assessments, the requirements for a rebuttable presumption, and the requirements for an affirmative defense.

Wilson Sonsini Goodrich & Rosati routinely helps companies navigate complex privacy and data security issues and monitors AG guidance, enforcement, and litigation involving AI legislation to stay current on compliance issues. For more information or advice concerning your CAIA compliance efforts, please contact [Maneesha Mithal](#), [Chris Olsen](#), [Stacy Okoro](#), or any member of the firm's [privacy and cybersecurity practice](#).

Wilson Sonsini's AI Working Group assists clients with AI-related matters. Please contact [Maneesha Mithal](#), [Laura De Boel](#), [Manja Sachet](#), or [Scott McKinney](#) for more information.

^[1]“Person” means “an individual, corporation, business trust, estate, trust, partnership, unincorporated association, or two or more thereof having a joint or common interest, or any other legal or commercial entity.”

^[2]For additional guidance on the current Artificial Intelligence Risk Management Framework released by NIST in January 2023, please read our client alert outlining the framework [here](#). Please also see NIST's supplemental guidance on generative AI [here](#).