

Alert 20 June 2024 | 9 min read

Newly passed Colorado AI Act will impose obligations on developers and deployers of high-risk AI systems

Hope Anderson | Ilesha Nunes | John Oltean

The Colorado Artificial Intelligence Act will impose mounting obligations on developers and deployers of high-risk AI systems in an effort to protect consumers from discriminatory consequential decisions by such systems.

On May 17, 2024 Colorado enacted the first comprehensive artificial intelligence (AI) legislation in the United States – the Colorado AI Act (the "**Act**") – which will go into effect in February 2026. Among other obligations, the Act creates duties for developers and deployers 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 "high-risk AI systems."¹ A "high-risk AI system" is a system that makes or is a substantial factor in making a "consequential decision," which 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:

- Education enrollment or opportunity
- Employment or an employment opportunity
- A financial or lending service
- An essential government service
- Healthcare services
- Housing

- Insurance
- Legal services²

"Algorithmic discrimination" includes any use of a high-risk artificial intelligence system that results in "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 [Colorado] or federal law."³

Pursuant to the Act, a "developer" is an individual, corporation, or other legal or commercial entity doing business in Colorado⁴ that "develops or intentionally and substantially modifies" an AI system.⁵ A "deployer" is an individual, corporation, or other legal or commercial entity doing business in Colorado that deploys a high-risk AI system.⁶

Deployers must conduct impact assessments under the Act

Deployers of high-risk AI systems must complete annual impact assessments for such systems.⁷ The required annual impact assessment must include the following information:

- A statement disclosing the purpose(s), intended use cases, deployment context and benefits of the high-risk AI system
- An analysis of whether deployment of such system poses any known or reasonably foreseeable risks of algorithmic discrimination, and if so, details on such discrimination and any mitigations that have been implemented
- A description of the data categories processed as inputs and the outputs produced
- If the deployer used data to customize the high-risk AI system, an "overview" of the categories of data used for customization
- Any metrics used to evaluate the performance and known limitations of the high-risk AI system
- A description of any transparency measures taken with respect to the high-risk AI system, including any measures taken to notify Colorado consumers when the system is being utilized

- A description of the post-deployment monitoring and user safeguards, including oversight, use and learning processes established by the deployer to address any issues⁸

Notably, deployers can contract out these assessment and reporting obligations to a third party.⁹ Moreover, a single impact assessment may be sufficient to address "a comparable set of high-risk artificial intelligence systems."¹⁰ Finally, a deployer that conducts an impact assessment for complying with another applicable law or regulation may be able to avoid conducting a separate impact assessment under the Colorado AI Act "if the impact assessment is reasonably similar in scope and effect" to the one contemplated therein.¹¹

Deployers must maintain all impact assessments and the records associated with them "for at least three years following the final deployment of the high-risk artificial intelligence system."¹² The Colorado Attorney General may require that a deployer (or a third party contracted by the deployer) provide such impact assessments and associated records within 90 days of a request in a form and manner prescribed by the Colorado Attorney General. However, notably, the Act expressly provides that the impact assessments and associated records are not subject to disclosure under the Colorado Open Records Act, and that the provision of such documents to the Colorado Attorney General shall not constitute a waiver of attorney-client privilege or work-product protection.

Developers and deployers must also comply with consumer transparency requirements

The Colorado AI Act requires that deployers and developers providing any consumer-facing AI system (this obligation is not limited to "high-risk" AI systems) ensure that they provide consumer-facing disclosures informing users that are interacting with such AI systems, unless the interaction "would be obvious to a reasonable person."¹³

Moreover, if a deployer uses a high-risk AI system to make an adverse consequential decision concerning a consumer, it must send the affected consumer a notice that includes the following information:

- A disclosure of the principal reason(s) for the consequential decision, including:
 - The degree/manner in which the high-risk AI system contributed to the decision
 - The type of data processed to make the decision
 - The source or sources of such data
- An opportunity to correct any incorrect personal data that factored into the decision
- An opportunity to appeal any adverse decision, which appeal must allow for human review¹⁴

Such notice is subject to certain exceptions, but must generally be provided directly to the consumer, in plain language, and in a format that is accessible to consumers with disabilities.¹⁵

Deployers and developers have incident reporting obligations

Developers must disclose any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of a high-risk AI system to the Colorado Attorney General and to all known deployers or other developers of the system within 90 days if: (i) the developer discovers the system has been deployed and has caused or is reasonably likely to have caused algorithmic discrimination; or (ii) the developer receives a credible report from a deployer that the system has caused algorithmic discrimination.¹⁶

Deployers have similar incident reporting obligations, as they must notify the Colorado Attorney General that a high-risk AI system they have deployed has caused algorithmic discrimination within 90 days after making such a discovery.¹⁷

Developers and deployers face additional obligations under the Act

While developers and deployers have several joint responsibilities, the Act also imposes separate obligations on both. However, if a developer or deployer has complied with all of the Act's substantive obligations, there is a rebuttable presumption that a developer or deployer used reasonable care to avoid discriminatory decisions via a high-risk AI system.¹⁸

Developers' obligations

Developers have stringent obligations under the Act, which require that developers "make available" a packet of disclosures and documentation to deployers to avoid liability for reasonably foreseeable discriminatory impacts of high-risk AI systems.¹⁹ The packet must include:

- A general statement describing the "reasonably foreseeable uses and known harmful or inappropriate uses" of the system
- Documentation disclosing:
 - High-level summaries of the type of data used to train the system
 - Any known or foreseeable limitations of the system, including risks of algorithmic discrimination from intended uses
 - The purpose and intended benefits and uses of the system
 - Any other information necessary for the developer to meet its obligations under the Act
- Documentation describing:
 - How the system was evaluated for performance and mitigation of algorithmic discrimination
 - Data governance measures used to cover the training datasets and to examine the "suitability" of data sources, biases and mitigation
 - The intended outputs of the system
 - How the system should be used, not be used, and monitored by an individual when used to make (or as a substantial factor in making) a consequential decision
 - Any additional information necessary to assist a deployer in understanding the system and risks for algorithmic discrimination²⁰

The Act also imposes several additional obligations on developers. Developers must:

- Make documentation and information available to deployers through "artifacts such as model cards, dataset cards, or other impact assessments" necessary for deployers to complete an impact assessment pursuant to the Act

- Include a clear, regularly updated and "readily available" statement on their website summarizing:
 - The types of high-risk AI systems the developer has developed or intentionally and substantially modified and currently makes available
 - How the developer manages known or reasonably foreseeable risks of algorithmic discrimination arising from the systems²¹

Deployers' Obligations

Like developers, deployers also face specific obligations under the Act. Importantly, deployers must implement a risk management policy and program that:

- Specifies and incorporates the principles, processes and personnel used to identify, document and mitigate foreseeable risks of algorithmic discrimination
- Is aligned with existing standards including the National Institute of Standards and Technology's AI Risk Management Framework and the International Organization for Standardization's ISO 42001
- Is regularly reviewed and updated²²

Enforcement

The Colorado Attorney General has exclusive enforcement authority to address violations of the Colorado AI Act, which will constitute unfair trade practices under Colo. Rev. Stat. § 6-1-105.²³ Punishments can include fines or injunctive relief. The Colorado AI Act provides for no private right of action.

Key takeaways

- **Important precedential effect:** The Act represents the first comprehensive AI legislation in the US, and other states are likely to follow suit if the federal government cannot move quickly to pass a comprehensive nationwide AI bill. However, Colorado's governor, Jared Polis, has been tepid in his support of the Act, encouraging Colorado legislators to consider amendments to avoid undue impact on helpful AI applications.

In any event, the Act—even if ultimately amended—may spur significant movement on AI regulation across the US. In fact, California (among other states) already has several AI-related bills under review.

- **Imposes stringent obligations:** Deployers and developers alike are required to comply with several detailed obligations within the Act, necessitating a careful review of the impact of AI systems.
- **Requires consumer transparency:** Deployers and developers must disclose the reason(s) behind adverse consequential decisions and then allow consumers to correct inaccuracies or appeal any such adverse decisions. These requirements provide consumers with more control over automated systems that may make impactful decisions about them. Additionally, deployers and developers must provide users with public-facing disclosures when they are interacting with AI.
- **Incident disclosure requirement:** Developers and deployers must disclose any foreseeable or actual algorithmic discrimination by a high-risk AI system to the Colorado Attorney General, who has exclusive authority to enforce the Act.

White & Case will continue to closely track any new developments on AI regulation in the US. For more information, please visit our AI Watch: Global Regulatory Tracker page.

1 Colo. Rev. Stat. §§ 6-1-1702.1, 6-1-1703.1.

2 Colo. Rev. Stat. §§ 6-1-1702.3, 6-1-1702.9.

3 Colo. Rev. Stat. §§ 6-1-1701.1.

4 The concept of "doing business in Colorado" is not defined in the Act. The Colorado Department of Revenue suggests that businesses without a physical location in Colorado are "doing business in Colorado" if they "solicit business and receive orders from Colorado residents by any means whatsoever." Accordingly, we expect this phrasing to be interpreted broadly; however, the Act empowers the Colorado Attorney General to promulgate rules, as necessary, for the purpose of implementing and enforcing the Act, so a narrower scope of applicability may be applied prior to the February 2026 effective date.

5 Colo. Rev. Stat. § 6-1-1702.7.

6 Colo. Rev. Stat. § 6-1-1702.6.

7 Colo. Rev. Stat. § 6-1-1703.3.

8 Colo. Rev. Stat. § 6-1-1703.3(b).

9 Colo. Rev. Stat. § 6-1-1703.3(a)(l).

10 Colo. Rev. Stat. § 6-1-1703.3(d).

11 Colo. Rev. Stat. § 6-1-1703.3(e).

12 Colo. Rev. Stat. § 6-1-1703.3(f).

13 Colo. Rev. Stat. § 6-1-1704.

14 Colo. Rev. Stat. § 6-1-1703.4(b).

15 Colo. Rev. Stat. § 6-1-1703.4(c).

16 Colo. Rev. Stat. § 6-1-1702.5.

17 Colo. Rev. Stat. § 6-1-1703.7.

18 Colo. Rev. Stat. §§ 6-1-1702.1, 6-1-1703.1.

19 Colo. Rev. Stat. § 6-1-1702.2.

20 Colo. Rev. Stat. § 6-1-1702.2.

21 Colo. Rev. Stat. § 6-1-1702.3(a).

22 Colo. Rev. Stat. § 6-1-1703.2.

23 Colo. Rev. Stat. § 6-1-1706.

White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

This article is prepared for the general information of interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.

