BLANKROME

Privacy, Security & Data Protection

JUNE 4, 2024

Colorado Becomes the First State to Enact Comprehensive AI Legislation

Colorado recently became the first U.S. state to enact its own comprehensive artificial intelligence ("AI") legislation, SB 24-205 (the "Colorado AI Act" or "Act"). The Colorado AI Act applies to all "developers" and "deployers" of "high-risk artificial intelligence systems" that do business in Colorado, without any other applicability thresholds, and aims to protect all Colorado residents, including employees. The Act, which will take effect on February 1, 2026, imposes obligations relating to transparency and preventing algorithmic discrimination, requiring differing obligations for developers and deployers. In preparation, companies doing business in Colorado should assess whether any high-risk AI systems are being developed or used or will be developed or used by the company and take appropriate action to meet the Act's requirements.

1. KEY DEFINITIONS

The Act defines "artificial intelligence systems" or "AI systems" as any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations that can influence physical or virtual environments.

"High-risk artificial intelligence systems" or "high-risk AI systems" are defined as any AI system that, when deployed, makes, or is a substantial factor in making a consequential decision. High-risk AI systems exclude those that are intended to (i) perform narrow procedural tasks; or (ii) detect decision-making patterns or deviations from prior decision-making patterns and are not intended to replace or influence human assessment or review. The statute also excludes certain technologies, such as anti-fraud, anti-malware, anti-virus, firewalls, cybersecurity software, and spam filtering, when they are not a substantial factor in making consequential decisions.

"Consequential decisions" are decisions that have a material legal or similarly significant effect on the provision or denial to any Colorado resident ("consumer") of, or the cost or terms of: (a) education enrollment or opportunity; (b) employment or employment opportunity; (c) financial or lending services; (d) essential government services; (e) healthcare services; (f) housing; (g) insurance; and (h) legal services.

"Developers" are those doing business in Colorado that develop or intentionally and substantially modify an AI system.

"Deployers" are those doing business in Colorado that deploy a high-risk AI system.

"Algorithmic discrimination" means 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 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 laws. However, algorithmic discrimination excludes discrimination that may result from the use of a high-risk AI system for the sole purpose of self-testing their own systems to identify and rectify incidents or risks of discriminatory behavior/outputs or expanding an applicant, customer, or participant pool to increase diversity or redress historical discrimination.

2. DEVELOPERS V. DEPLOYERS

The Colorado AI Act requires developers and deployers of high-risk AI systems to use reasonable care to protect consumers from any known or foreseeable risks of algorithmic discrimination arising from the intended and contracted uses of the high-risk AI systems. Compliance with the Act's requirements and any additional requirements that the Colorado Attorney General may adopt through regulations creates a rebuttable presumption that reasonable care was used. Both developers and deployers are subject to compliance audits by the Colorado Attorney General.

The Act also contains an AI incident reporting obligation. Developers are required to report to the Attorney General any known or reasonably foreseeable risks of algorithmic discrimination in connection with a high-risk AI system. A deployer is required to report to the Attorney General if it discovers a high-risk AI system it has deployed has caused algorithmic discrimination. In each case, reports must be made to the Attorney General within 90 days of discovering such discrimination or risk of discrimination. Developers have the additional obligation of notifying all known deployers and other developers of the high-risk AI system.

Companies using high-risk AI systems are also subject to a number of transparency, disclosure, reporting, and other obligations depending on their role as a developer or deployer.

Developer Obligations

Developers must:

- Make available to deployers or other developers of the high-risk AI system a **general statement** describing the reasonably foreseeable uses and known harmful or inappropriate uses of the high-risk AI system.

- Make available to deployers or other developers of the high-risk AI system **documentation** that discloses, among other things, a high-level summary of the type of data used to train the high-risk AI system, data governance measures used to cover the training data sets and measures used to examine the suitability of data sources, possible biases and appropriate mitigation, and information intended to aid deployers and other developers in using and assessing risk associated with the high-risk AI system.

  Information required to be provided by developers to aid in use and risk management includes information on the purpose of the high-risk AI system, the intended outputs of the high-risk AI system, and all other information necessary to assist deployers in completing impact assessments, to allow the deployer to comply with its obligations, and to assist the deployer in understanding the outputs and monitor the performance of the high-risk AI system for risks of algorithmic discrimination.

- Provide all information and documents to deployers **to assist deployers in completing impact assessments.**

- Provide a **notice** on its website or in a public use case inventory that summarizes: (i) the types of high-risk AI systems developed or intentionally and substantially modified by the developer; and (ii) how the developer manages known or reasonably foreseeable risks of algorithmic discrimination that may arise for the development or intentional and substantial modification of the high-risk AI systems.

Deployer Obligations

Deployers must, with limited exceptions:

- Implement, maintain, and regularly review and update a **risk management policy and program** that is used to identify, document, and mitigate known or reasonably foreseeable risks of algorithmic discrimination. The Colorado AI Act references AI Risk Management Framework ("RMF") guidance from the National Institute of Standards and Technology ("NIST") and other standards as tools that can be used to assess reasonableness. The size and complexity of the organization; the nature, scope, and intended use of the high-risk systems; and the sensitivity of the data processed in connection with the use of high-risk systems are also factors to consider when assessing whether a deployer's risk management policy and program are reasonable.

- Complete an **impact assessment** for each high-risk AI system deployed at least annually and within 90 days after any intentional and substantial modification to the high-risk AI system is made available. The impact assessment must be retained for three years following the final deployment of the high-risk AI system. The Act requires specific information be provided in each impact assessment, including (a) a statement disclosing the purpose, intended use cases, deployment context, and benefits of the high-risk AI system; (b) an analysis of whether the deployment of the high-risk AI system poses any known or reasonably foreseeable risks of algorithmic discrimination, along with mitigating steps taken; and (c) a description of post-deployment monitoring

and user safeguards, including the oversight, use, and learning process the deployer established to address issues resulting from the deployment of the high-risk AI system, among other things.

- **Review** the deployment of each high-risk AI system at least annually to ensure that the high-risk AI system is not causing algorithmic discrimination.

- Provide **notices to consumers** on its website containing specific disclosures.

- Provide consumers the **rights** provided by the Colorado Privacy Act and the right to appeal an adverse consequential decision.

3. ENFORCEMENT

Violations of the Colorado AI Act constitute an unfair trade practice under state law. However, the Act provides several affirmative defenses for violations, including complying with the latest RMF published by NIST or another substantially equivalent nationally recognized risk management framework for AI systems or any risk management framework for AI systems that the Colorado Attorney General may designate.

The Act does not provide for a private right of action and instead provides the Colorado Attorney General with exclusive enforcement authority. The Colorado Attorney General also has the authority to issue rules as necessary for the purpose of implementing and enforcing the Act.

4. KEY TAKEAWAYS

With over a quarter of U.S. state legislatures having considered some form of AI regulation in the last year, the Colorado AI Act as well as the European Union's AI Act may spur other states to push through AI laws over the next few years much like states have passed comprehensive data privacy legislation since the passage of the California Consumer Privacy Act in 2018. Companies doing business in Colorado, in preparation of the Colorado AI Act, should:

- Identify whether any high-risk AI systems are being developed or used or will be developed or used by the company (*i.e.,* any AI systems that make or are a substantial factor in making "consequential decisions"). As stated above, this can include common use cases such as decisions affecting employment or an employment opportunity;

- Develop or update existing AI governance policies and procedures to comply with a nationally or internationally recognized AI risk management framework;

- Draft and implement a risk management policy and program if deploying a high-risk AI system;

- Prepare requisite public-facing notices on the development or use of a high-risk AI system;

- Establish processes for detecting and mitigating algorithmic bias arising from use of high-risk AI systems;

- Establish processes for complete impact assessments, if deploying a high-risk AI system;

- Establish processes to notify the Colorado Attorney General of algorithmic discrimination caused or reasonably likely caused by a high-risk AI system; and

- Keep an eye out for rules that may be issued by the Colorado Attorney General.

For further information and assistance, contact Sharon R. Klein, Alex C. Nisenbaum, Karen H. Shin, or another member of Blank Rome's Privacy, Security & Data Protection group.

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Alex C. Nisenbaum
949.812.6011 | alex.nisenbaum@blankrome.com

Karen H. Shin
949.812.6012 | karen.shin@blankrome.com