Navigating New Frontiers: Colorado's Groundbreaking AI Consumer Protection Law

31 May 2024

Privacy + Data Security

Client Alert

The **Colorado Act Concerning Consumer Protections in Interactions with Artificial Intelligence Systems** (the "**Colorado AI Act**" or the "**Act**") is the first of its kind in the United States. It introduces comprehensive consumer protection measures targeting interactions with AI systems. This pioneering legislation, set to take effect on February 1, 2026, places new obligations on developers and deployers of high-risk AI systems, including enhanced transparency requirements and various consumer rights. The Colorado AI Act is similar to the EU AI Act, for example, in applying a risk-based approach to regulating AI. However, there also are several differences, such as the Colorado AI Act's more limited territorial scope and more extensive requirements for deployers of high-risk AI systems. For more detail on the similarities and differences, see **Colorado AI Act vs EU AI Act**.

Key Takeaways

If your company does business in Colorado and either develops or deploys AI systems:

- Determine whether the systems qualify as high-risk AI systems under the Act and incorporate questions to assess into the review of new systems.
- Review AI governance and documentation practices to determine how to comply with the transparency and documentation requirements and whether any existing governance and compliance frameworks may be leveraged for the new requirements.
- Consider whether any individual rights processes must be updated to address consumer rights under the Colorado AI Act, including the right to appeal.

Scope

The Colorado AI Act will apply to developers and deployers. Developers are persons doing business in the state that develop or intentionally and substantially modify an AI system, while deployers are persons doing business in the state that deploy a *high-risk* AI system. Unlike many of the state consumer privacy laws, the Colorado AI Act does not have a threshold number of consumers to trigger applicability. And while both the Colorado AI Act and the Colorado Privacy Act (**CPA**) use "consumers," the term refers to Colorado residents under the AI Act and the CPA defines consumers as Colorado residents "acting only in an individual or household context," excluding anyone acting in a commercial or employment context. Therefore, companies that may not be subject to the CPA may have obligations under the Colorado AI Act.

High-risk AI Systems

Similar to the EU AI Act (see our alert—**EU AI Act – Landmark Law on Artificial Intelligence Approved by the European Parliament**), the bulk of the Colorado AI Act's requirements apply to "high-risk AI systems." These are defined as any artificial intelligence system that, when deployed, makes or is a substantial factor in making consequential decisions. Consequential decisions are those with a **material legal** or **similarly significant** effect on the provision or denial to any Colorado resident of, or the cost or terms of:

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

Contacts

Marian A. Waldmann Agarwal
mwaldmann@mofo.com
(212) 468-7900
(212) 336-4230
Marijn Storm
mstorm@mofo.com
32 23407364
32-2-347-1824

About Morrison Foerster

We are Morrison Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, and Fortune 100, technology, and life sciences companies. The Financial Times has named us to its list of most innovative law firms in North America every year that it has published its Innovative Lawyers Reports in the region,and Chambers Asia-Pacific has named us the Japan International Firm of the Year for the sixth year in a row. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger.

- **Insurance**

- A **legal** service

While this definition does not completely align with the EU AI Act's high-risk artificial systems, there are overlapping areas of concern that are relevant to many companies. For example, the EU AI Act also recognizes the risks related to using AI Systems for decisions related to education, employment, and healthcare as high-risk areas.

Duties of Developers and Deployers of High-Risk AI Systems

The Colorado AI Act requires developers and deployers of these high-risk AI systems to use "reasonable care" to avoid algorithmic discrimination and establishes specific requirements for what constitutes reasonable care. Algorithmic discrimination is defined as "the use of an artificial intelligence system [that] results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of an actual or perceived" classification status protected by Colorado or federal law. Compliance with the requirements of the Colorado AI Act creates a rebuttable presumption that a developer or deployer used reasonable care to avoid algorithmic discrimination. An overview of the main requirements for deployers and developers is included below.

Obligations imposed on **developers** of high-risk AI systems include the following:

- **Documentation and risk assessment obligations:** Developers must make available to a deployer **information** and **documentation**, including high-level summaries of data used to train the system, information on uses, risks of algorithmic discrimination, methods used to evaluate and mitigate algorithmic discrimination risks, and information necessary for the deployer to comply with its obligations (including completing impact assessments);

- **Public documentation obligations:** Developers must make a **publicly available statement** summarizing the types of high-risk AI systems they have developed or intentionally and substantially modified and currently make available to deployers and how the developer manages any known or reasonably foreseeable risks of algorithmic discrimination that may arise from the development or intentional and substantial modification of each of these systems; and

- **Notification obligations:** Developers must **disclose to the Attorney General** and known deployers any **known or reasonably foreseeable risk of algorithmic discrimination**, within 90 days after the discovery or receipt of a credible report from the deployer, that the high-risk AI system has caused or is reasonably likely to have caused.

Obligations imposed on **deployers** of high-risk AI systems include the following:

- **Assessment obligations:** Deployers must implement a **risk management policy and program**; complete an **impact assessment**; and **review,** at least annually, each deployment to ensure that the high-risk system is not causing algorithmic discrimination;

- **Consumer rights obligations:** Deployers must **notify consumers** of specified items if the high risk system makes a consequential decision concerning that consumer; provide consumers with an opportunity to **correct** errors in personal data that a high-risk AI system processed in making a consequential decision; and provide Colorado residents with an opportunity to **appeal**, via human review if technically feasible, an adverse consequential decision concerning the resident arising from a high-risk AI system's deployment;

- **Public documentation obligations:** Deployers must make a **publicly available statement** summarizing the types of high-risk systems that the deployer currently deploys; how the deployer manages any known or reasonably foreseeable risks of algorithmic discrimination that may arise from deployment of each of these high-risk systems; and the nature, source, and extent of the information collected and used by the deployer; and

- **Notification obligations***:* Deployers must **disclose to the Attorney General** the discovery of **algorithmic discrimination**, within 90 days after the discovery, that the high-risk system has caused or is reasonably likely to have caused.

Other Obligations

In addition to the obligations above, deployers or developers that deploy, offer, sell, lease, license, give, or otherwise make available an AI system that interacts directly with consumers must inform consumers that they are interacting with an AI system, unless it would be obvious to a reasonable person.

Exemptions

The Colorado AI Act provides for some limited exemptions, including for:

- HIPAA covered entities making certain non-high-risk healthcare recommendations generated by AI that require a provider to take action to implement;
- Insurers subject to CO Section 10-3-1104.9 and related rules;
- AI systems acquired by the federal government or federal agencies, etc.; and
- Certain banks and credit unions that are subject to substantially similar or stricter guidance or regulations applicable to the use of high-risk AI systems and that require, at a minimum, regular audits of such systems and the mitigation of any algorithmic discrimination caused by use or risk that is reasonably foreseeable to result from the use of the high-risk AI system.

Enforcement

The Attorney General has exclusive authority to enforce the Colorado AI Act as well as rule-making authority. Violations of the Colorado AI Act's provisions constitute a deceptive trade practice. There is no private right of action.

Developers, deployers, and other persons have an affirmative defense to any action brought by the Attorney General if they:

- Discover and cure a violation because of feedback, adversarial testing, or red-teaming (as defined by the National Institute of Standards and Technology (**NIST**)) or an internal review process; **and**
- Are otherwise in compliance with the latest version of **NIST's Artificial Intelligence Risk Management Framework** or certain other risk management frameworks if substantially equivalent to the law or more stringent or if designated by the Attorney General.

Colorado AI Act and Colorado Privacy Act

Use of high-risk AI systems will likely also be profiling under the CPA where consumer (as defined by the CPA) personal data is processed. Entities subject to the CPA must provide consumers with notice of profiling and the right to opt out at or before any profiling in furtherance of decisions that produce legal or similarly significant effects concerning the resident. In addition, companies subject to the CPA must conduct and document a data protection assessment if the profiling presents a reasonably foreseeable risk to consumers of: (i) unfair or deceptive treatment, or unlawful disparate impact; (ii) financial or physical injury; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, if the intrusion would be offensive to a reasonable person; or (iv) other substantial injury.

Colorado AI Act vs EU AI Act

The Colorado AI Act is similar to the EU AI Act in a few ways. For example, both take a risk-based approach to regulating AI and require assessment and management of AI risks. There are, however, also several differences, such as the more limited territorial scope of the Colorado AI Act and the fact that it imposes more significant requirements on deployers of AI systems. The table below summarizes some of these differences:

	Colorado AI Act	EU AI Act
Territorial scope	Focuses on the protection of Colorado residents and imposes requirements on developers and deployers doing business in Colorado.	Applies across the EU and also applies to developers or deployers not established in the EU if they make an AI system available on the EU market or if the output of the AI system is used in the EU.

	Colorado AI Act	EU AI Act
Qualification of high-risk AI systems	Overlaps in areas of education, employment, financial services, government services, but—in addition to the EU AI Act—Colorado also includes AI systems in housing or legal services.	Also includes AI systems in biometrics, emotion recognition, law enforcement, migration and border control, democratic processes and administration of justice, and AI systems that are safety components in, or themselves covered by, existing EU product safety legislation.
Requirements for deployers	A significant number of requirements are imposed on deployers.	Most of the risk-management requirements for high-risk AI systems are imposed on providers rather than deployers.
Notice to consumers and right to appeal	Requires transparency toward individuals and the right to appeal adverse consequential decisions that arise from the deployment of an AI system.	Requires the explanation of decisions made based on high-risk AI outputs. Transparency by providers to deployers and human oversight is required. However, transparency and appeal rights apply under the EU General Data Protection Regulation if personal data is used.
General-purpose AI models (e.g., generative AI)	No specific requirements for general-purpose AI models.	Specific requirements for providers of general-purpose AI models, including a requirement to publish a summary of the content used to train the model.
Penalties	Violations qualify as an unfair trade practice that is subject to penalties of up to $20,000 for each violation, with a violation considered a separate violation for each consumer or transaction involved.	Allows significant penalties to be imposed of up to EUR 35 million or 7% of total worldwide revenue.