

---

## Understanding Colorado's Landmark AI Legislation and Its Impact on Businesses

---

June 10, 2024

**Coraleine Kitt**

*Reprinted with permission from the June 10, 2024 edition of The Legal Intelligencer. 2024 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-256-2472 or [asset-and-logo-licensing@alm.com](mailto:asset-and-logo-licensing@alm.com).*

The landscape of artificial intelligence (AI) regulation in the United States is evolving rapidly, with Colorado emerging as a pioneer in consumer protection measures with the Colorado Act Concerning Consumer Protections in Interactions with Artificial Intelligence Systems (the Colorado AI Act). This act, the first of its kind in the country, aims to reshape AI system deployment and development, setting a precedent for other jurisdictions. Scheduled to take effect on February 1, 2026, the Colorado AI Act introduces a comprehensive framework aimed at addressing the potential risks associated with AI systems, particularly those making consequential decisions affecting consumers.

### **Scope and Applicability**

The Colorado AI Act has broad scope, encompassing both developers and deployers of AI systems within the state. Developers refer to entities conducting business in Colorado engaged in the development or substantial modification of AI systems. Deployers are defined as entities operating within Colorado that deploy high-risk AI systems. Additionally, the scope of the Colorado AI Act extends to interactions with AI systems that have a material legal or similarly significant effect on various aspects of consumers' lives, including education, employment, financial services, government services, healthcare, housing, insurance, and legal services. Unlike some consumer privacy laws, the Colorado AI Act does not establish a minimum threshold of consumers for its applicability, meaning that entities of any size engaging in covered activities are included. The Act applies to interactions involving AI systems that have a material legal or similarly significant effect on various aspects of consumers' lives, including education, employment, financial services, government services, healthcare, housing, insurance, and legal services. The term "consumer" refers specifically to Colorado residents.

Central to the Colorado AI Act is the classification of "high-risk AI systems," which includes AI systems involved in making consequential decisions across various domains such as education, employment, finance, healthcare, housing, insurance, and legal services. These decisions are characterized by their significant impact on individuals' rights, opportunities, and access to essential services. By targeting high-risk systems, the legislation aims to mitigate potential harms, such as algorithmic discrimination, that may arise from automated decision-making processes.

### **Duties of Developers and Deployers**

*Continued*

---

Under the Colorado AI Act, developers of high-risk AI systems are subject to several duties aimed at promoting transparency, accountability, and the prevention of algorithmic discrimination. For example, developers must provide deployers with comprehensive documentation, including high-level summaries of the data used to train the system, information on uses and risks of algorithmic discrimination, methods for evaluating and mitigating algorithmic discrimination risks, and any information necessary for deployers to fulfill their obligations, such as completing impact assessments. Developers are also required to make publicly available statements summarizing the types of high-risk AI systems they have developed or substantially modified, along with how they manage known or foreseeable risks of algorithmic discrimination associated with these systems. These statements must be regularly updated to reflect any changes or developments. In the event of known or reasonably foreseeable risks of algorithmic discrimination, developers must disclose this information to the Colorado Attorney General and known deployers within 90 days after discovery or receipt of a credible report from a deployer indicating that the high-risk AI system has caused or is likely to cause algorithmic discrimination.

Deployers, on the other hand, have several key duties aimed at ensuring responsible use of AI systems and safeguarding against algorithmic discrimination. For example, deployers must implement a comprehensive risk management policy and program to govern the use of high-risk AI systems. This includes conducting impact assessments to evaluate the potential risks of algorithmic discrimination associated with the deployment of these systems. Additionally, deployers are required to notify consumers if a high-risk AI system makes a consequential decision regarding them. This notification must include information about the purpose of the AI system, the decision made, and the consumer's right to correct any errors in personal data used by the system and appeal adverse decisions. Further, deployers must make publicly available statements summarizing the types of high-risk systems they deploy, how they manage risks of algorithmic discrimination associated with these systems, and the nature, source, and extent of the information collected and used by the deployer. Deployers also must disclose to the Colorado Attorney General any instances of algorithmic discrimination discovered within 90 days of the discovery. This requirement ensures that any discriminatory outcomes resulting from the deployment of high-risk AI systems are promptly reported and addressed.

### **Exemptions and Enforcement**

While the Colorado AI Act imposes stringent requirements on developers and deployers, it provides several exemptions aimed at certain entities and scenarios.

The Colorado AI Act exempts HIPAA covered entities when making certain non-high-risk healthcare recommendations generated by AI that require a healthcare provider to implement the recommendation. This exemption acknowledges the existing regulatory framework governing healthcare data privacy and ensures alignment with HIPAA requirements.

Insurers subject to CO Section 10-3-1104.9 and related rules are also exempt from certain provisions of CAIA. This exemption recognizes the unique regulatory landscape governing the insurance industry and the need to avoid duplicative or conflicting obligations.

*Continued*

---

Additionally, AI systems acquired by the federal government or federal agencies are exempt from CAIA's requirements. This exemption acknowledges the federal government's authority to regulate AI systems within its purview and ensures consistency with federal regulations.

Certain banks and credit unions subject to substantially similar or stricter guidance or regulations applicable to the use of high-risk AI systems are exempt from certain provisions of CAIA. This exemption recognizes existing regulatory oversight in the financial sector and aims to avoid regulatory redundancy.

The enforcement of the Colorado AI Act is primarily entrusted to the Colorado Attorney General's office. In the event of non-compliance, violations of the Colorado AI Act 's provisions are considered deceptive trade practices, subject to civil penalties. These penalties can amount to a maximum of \$20,000 for each violation, with each violation being assessed on a per-consumer or per-transaction basis. The Colorado AI Act does not provide for a private right of action, meaning that enforcement actions can only be initiated by the Colorado Attorney General. Additionally, the Colorado AI Act empowers the Attorney General's office to promulgate rules across various domains, including documentation, notices, disclosures, impact assessments, and risk management policies and programs.

#### **Colorado AI Act vs EU AI Act**

The Colorado AI Act and the EU AI Act share common objectives of regulating AI to protect consumer interests, but they also exhibit some differences.

The Colorado AI Act primarily focuses on interactions within the state of Colorado, applying to developers and deployers operating within its jurisdiction. In contrast, the EU AI Act has a broader territorial scope, extending its reach to developers and deployers outside the EU if their AI systems are available on the EU market or their outputs affect EU residents. This key difference reflects the EU's global regulatory ambitions compared to the more localized scope of the Colorado AI Act.

While both acts recognize the risks associated with high-risk AI systems, they differ in their categorization criteria. The Colorado AI Act defines high-risk AI systems based on their potential to influence consequential decisions in various domains such as education, employment, and healthcare. Conversely, the EU AI Act includes additional high-risk categories such as biometrics, emotion recognition, law enforcement, and democratic processes. This broader classification under the EU AI Act reflects its comprehensive approach to identifying and regulating AI risks.

Both acts impose obligations on developers and deployers, albeit with some variations. The Colorado AI Act mandates developers to exercise reasonable care to avoid algorithmic discrimination, accompanied by stringent documentation and disclosure requirements. Deployers are required to implement risk management policies, conduct impact assessments, and ensure consumer rights, including the right to appeal adverse decisions. In contrast, the EU AI Act places more emphasis on risk management requirements for providers rather than deployers. Additionally, while the Colorado AI Act focuses on transparency and consumer rights, the EU AI Act emphasizes explanations of decisions made by high-risk AI systems and mandates human oversight, particularly in sensitive areas.

*Continued*

---

Enforcement mechanisms differ between the two acts. The Colorado AI Act grants exclusive enforcement authority to the Colorado Attorney General, with violations constituting deceptive trade practices subject to civil penalties. In contrast, the EU AI Act empowers national supervisory authorities to enforce its provisions, with significant penalties of up to EUR 35 million or 7% of total worldwide revenue for non-compliance. This divergence in enforcement mechanisms reflects the varying regulatory frameworks and enforcement priorities of the respective jurisdictions.

### **Preparing for Compliance**

As this groundbreaking legislation takes effect on February 1, 2026, AI companies operating in Colorado should proactively assess their systems, enhance transparency, and implement robust governance frameworks to align with the new requirements. Focusing on addressing potential risks associated with AI, particularly in high-impact areas, can help mitigate harms such as algorithmic discrimination. Staying informed and preparing for compliance will ensure that companies meet the standards set forth by this pioneering regulation.

**Coraleine J. Kitt, CIPP/US, CIPP/E**, is a member of Flaster Greenbergs Intellectual Property Department and Patent Practice Group. She regularly provides strategic counselling on issues arising from the collection, use, sharing, and security of data, including when bringing new products to market, leveraging data in new ways, and complying with the CCPA, the GLBA, the GDPR, FTC requirements, and global digital marketing laws and frameworks. She also has substantial experience in creating and implementing privacy policies and programs.

### **ATTORNEYS MENTIONED**

Coraleine Kitt, CIPP/US, CIPP/E