BRITT
LAW

Your AI & Data Privacy Expert

PART 3 OF 6-PART SERIES

STATE ARTIFICIAL INTELLIGENCE LAWS

THIS IS THE THIRD OF A SIX-PART SERIES of commentaries on data management, authored by Steve Britt, managing partner of Britt Law LLC. These commentaries review the new laws and regulations relating to data privacy and artificial intelligence.

Steve is a deeply experienced **corporate and technology attorney** with world-class cyber, data privacy & artificial intelligence expertise, including three international data certifications. He also has extensive experience with software licensing, cloud, SaaS and data hosting. He practiced law in Washington, D.C. and Virginia prior to establishing Britt Law in Charleston, South Carolina. Steve formed Britt Law to leverage his data management experience and to offer a wider range of legal services with flexible fee arrangements. This includes fractional general counsel and fractional data protection engagements.

PART 3

INTRODUCTION

In the absence of federal legislation, states are enacting their own AI laws. This is taking place even though most of the new state data privacy laws already provide regulatory authority over AI algorithms. This means that the prospect of inconsistent state laws we have seen with data privacy is repeating itself for artificial intelligence.

The most noteworthy developments so far in this area (three statutes and one set of pending regulations) have occurred in Colorado, Utah and California.

COLORADO ARTIFICIAL INTELLIGENCE ACT

Colorado's AI Act was passed this year and will take effect on Feb. 1, 2026. It requires developers of high-risk AI systems to prevent algorithmic discrimination, the disparate treatment of individuals based upon their age, color, disability, ethnicity, race, religion and veteran status.

High-risk AI systems are those that make or substantially contribute to the making of a "consequential decision," which is any decision that affects the price or terms of access to education, employment, financial services, government services, healthcare, housing, insurance or legal services. The Act applies to such discrimination whether or not the system processed personal information.

The Act covers two categories of stakeholders: "developers," who build AI systems, and "deployers," who sell or license them, with or without modifications or enhancements by the deployer.

"Developers" must take the following actions:

I. Document the foreseeable proper and harmful uses of the AI system.

II. Explain the type and lineage of the training data used in the system.

III. Report on the logic of the algorithms and the mitigation measures implemented against algorithmic discrimination.

IV. Provide the information necessary for deployers to conduct their own impact assessments.

V. Publicly publish a statement detailing how the system was developed and how it manages known or foreseeable risks of discrimination.

VI. Promptly report to the Attorney General any instances of algorithmic discrimination.

"Deployers" share many of these same obligations. They must conduct annual impact assessments and must inform customers of their right to opt-out of the processing of their personal information for purposes of profiling them. Deployers must explain any adverse decisions by the system and provide the user with the right to appeal such decisions.

Given the expected costs of compliance, the Act exempts deployers with less than 50 full-time employees from having to implement risk management programs and annual impact assessments but does not exempt them from its other provisions.

Unlike the EU AI Act, the Colorado AI Act does not expressly cover general-purpose AI systems ("GPAI"). In fact, it excludes generative AI unless the technology is used to generate content, decisions, predictions or recommendations in support of consequential decisions.

The Colorado Act makes a strong push for the use of the NIST AI Risk Management Framework for the governance of AI systems. A violation of the AI Act constitutes a violation of Colorado's Unfair and Deceptive Trade Practices Act.

UTAH ARTIFICIAL INTELLIGENCE POLICY ACT

Utah was the first state to enact an artificial intelligence statute, which took effect on May 1, 2024. It is narrowly focused on the use of generative AI, which the Act subjects to Utah's consumer protection statutes.

Under the Act, a violation of a Utah consumer protection statute is not excused just because a generative AI system made the unlawful statement or committed the unlawful act.

There are two categories of disclosure obligations under the Act. The first is that a person using generative AI in connection with a business regulated by the Utah Division of Consumer Protection must disclose, if asked, that the user is interfacing with a machine. The other is that a person providing services of a licensed occupation, such as healthcare professionals, must affirmatively inform consumers in advance that they are interacting with AI.

The Act creates an Office of Artificial Intelligence Policy and an AI Learning Laboratory Program to facilitate the development of AI technologies. Companies accepted into the program can enter into a regulatory mitigation agreement with the state that reduces the regulatory burdens otherwise applicable to AI development.

Violations of the Utah AI Act may incur an administrative fine of up to $2,500 per violation by the Utah Division of Consumer Protection.

This statute is very narrow, so the main task for covered Utah companies is to implement a disclosure regime for the use of generative AI in regulated industries.

CALIFORNIA AI ACTS & CYBER, RISK ASSESSMENT & ADMT REGULATIONS

In 2024, the California legislature became very active on AI, passing six new laws. One (SB 1047) was vetoed by the governor, but three others are quite noteworthy, as described below:

I. **AB 2013 AI Training Data Transparency Act:** Effective on Jan. 1, 2026, this act requires developers of generative AI models to publicly post on their websites 12 specific pieces of information about the data used to train their systems. These disclosures include the sources of the datasets, the types of data points incorporated therein, any applicable IP rights to the data, whether the datasets contain personal information and a disclosure of any modifications to the model by the developer.

II. **SB 942 California AI Transparency Act:** Also effective on Jan. 1, 2026, this act applies only to generative AI systems that produce images or other audio or video content and reach 1,000,000 or more monthly users located anywhere. Providers subject to the Act must make an AI detection tool publicly and freely available to users that reveals when the system creates or alters any covered content. The user must also be given the information necessary to make appropriate disclosures to its users, including certain unique identifiers that are extraordinarily difficult to remove.

III. **AB 1008 Amendments to CCPA:** This bill amended the CCPA to cover personal information contained within AI system models if that data is capable of being output or extracted. This would grant data subject rights to the personal information inside the model itself, such as the tokens, model weights and other system data points. This will force developers to consider excluding personal information from their models, such as by de-identifying or aggregating the data or by using synthetic data. The California Privacy Protection Agency ("CPPA") supported passage of this bill, finding it "consistent with and reflective of existing law." Letter of CPPA Deputy Director of Policy and Legislation to CPPA Board, dated July 11, 2024.

The California Privacy Rights Act of 2020 ("CPRA") expanded the California Consumer Privacy Act ("CCPA"), creating the CPPA as the nation's only dedicated state data privacy regulator. The CPRA also directed the promulgation of regulations for activities that posed a significant risk to consumers' privacy or security, including requirements for:

i. Comprehensive and independent cybersecurity audits.

ii. Risk assessments for the processing of personal information.

iii. Regulation of the use of automated decision-making technologies ("ADMT").

The CPPA has drafted these regulations but and will soon promulgate them. They will incorporate most of the following requirements.

1. CYBERSECURITY AUDITS

Every business whose processing of personal information poses a significant risk to a consumer, and which meets a certain processing threshold, will be required to complete a cybersecurity audit. The initial audit is due 24 months after finalization of the regulations and updates to such audits are due annually thereafter.

Cyber audits must be performed by a qualified independent professional and must be reported to the board of directors or highest-ranking executive. They must assess the following controls:

- Authentication (including MFA and strong password policies)
- Encryption of personal information at rest and in transit
- Zero trust architecture
- Account management and access controls
- Secure configuration of hardware and software
- Vulnerability scans, penetration testing and network monitoring
- Cyber education and training
- Retention and disposal policies
- Security incident response management

If the business has had to make stakeholder incident notifications, a sample copy of those notifications must be included. The business must file with the CPPA a certification of its completion of the audit signed by a member of its board of directors or by its highest-ranking executive.

2. RISK ASSESSMENTS

Every business whose processing of personal information poses a significant risk to consumer privacy must also conduct a risk assessment. **"Significant risk to privacy"** is defined as (i) selling or sharing personal information, (ii) processing sensitive information, (iii) using automated decision-making technology (**"ADMT"**) for a significant decision or for extensive profiling, or (iv) using personal information to train ADMT or an AI system.

The risk assessment must balance the risks of the company's data processing activities against their benefits based on the purpose of the processing and any risk mitigation measures that have been implemented. The analysis must also explain any actions taken to maintain the quality of the data, the logic of the algorithms and the use of system outputs.

If the ADMT is provided to other entities, the developer must provide such recipients with the information necessary to understand the operations and limitations of the technology. Risk assessments must be conducted before a processing activity is initiated and after any material change to it. An abridged version of the assessment, including a certification of its proper completion, must be submitted to the CPPA.

3. ADMT REGULATIONS

A business that uses ADMT for **"significant decisions"** concerning a consumer relating to financial services, housing, insurance, education, employment, compensation, essential services or healthcare or for extensive profiling of the consumer must comply with the new ADMT regulations.

Any consumers subject to the outputs of ADMT must be provided a **"Pre-Use Notice"** explaining the purpose for the use of ADMT and the consumer's right to opt out of such use. Consumers must also be given an explanation of how the ADMT works, its logic, its intended outputs and how the business will use those outputs.

Consumers must be given a right to appeal any significant automated decision to a qualified human reviewer who has the authority to overturn the decision. Other rules apply to the use of ADMT in admission or hiring decisions, work assignments, compensation and work or education-related profiling.

If a consumer requests access to the ADMT action, the business must explain the purpose of its use of the technology, the output that was produced, how the business used the output and how the logic of the technology was applied to the consumer.

KEY TAKEAWAYS

- Since many of the AI development risks under state laws mirror those of the EU AI Act, you should review our "Key Takeaways" under our Part 2 commentary on the EU AI Act.
- With its comprehensive privacy and AI Acts, Colorado is taking a major role in the regulation of data and AI. Colorado's AI Act will apply to the use of AI systems even when personal information under its privacy act is not involved.
- The Utah AI Act deals with AI solely as a matter of consumer protection. Its requirement of the disclosure to consumers of the company's use of generative AI is a widely accepted obligation under all of the new laws
- California is headed for a groundbreaking regulation on cyber audits, risk assessments and automatic decision-making technologies. These regulations will accelerate the regulation of AI by other states.
- Just as a privacy impact assessment is the best means of implementing data privacy, you should incorporate AI governance principles into all AI development efforts and all data protection assessments.

To learn more, contact Steve Britt at steve@brittlawllc.com.