AN A.S. PRATT PUBLICATION
JULY-AUGUST 2024
VOL. 10 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 NUMBER 6 July-August 2024

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at .... (908) 673-3380
Email: .... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at .... (800) 833-9844
Outside the United States and Canada, please call .... (518) 487-3385
Fax Number .... (800) 828-8341
LexisNexis® Support Center .... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or .... (800) 223-1940
Outside the United States and Canada, please call .... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.
LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2024 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Utah and Colorado Have New Artificial Intelligence Laws

By Daniel K. Alvarez, Laura E. Jehl, Briony Pollard, Susan Rohol and Kari Prochaska*

In this article, the authors review Utah's Artificial Intelligence Policy Act and Colorado's first comprehensive state law regulating artificial intelligence.

On May 1, 2024, Utah's Artificial Intelligence (AI) Policy Act (the Utah AI Act) took effect. The Utah AI Act is the first U.S. state law to impose transparency obligations on companies using generative artificial intelligence (Gen AI). Those obligations are particularly critical for any company or individual in a regulated industry, such as medicine or accounting. Penalties are up to $2,500 for each violation, and the law may be enforced by the Utah Division of Consumer Protection or the courts.

Utah is not the only state making news on the AI policymaking front. On May 17, 2024, Colorado's governor signed into law Senate Bill 24-205, "Concerning Consumer Protections in Interactions with Artificial Intelligence Systems" (the Colorado AI Act). The Colorado AI Act, which becomes effective in February 1, 2026, leverages concepts from the European Union's Artificial Intelligence Act by introducing obligations for developers and deployers of high-risk AI systems and protections for consumers against algorithmic discrimination.

In addition, the Colorado Attorney General, under the authority of the Colorado Privacy Act, has adopted rules focused on the use of personal data in "automated processing," and the California Privacy Protection Agency (the CPPA) is likewise moving forward with rulemaking related to "automated decision-making." This is in addition to numerous state laws that have created task forces to study government use of AI, as well as various state bills that govern the use of AI in employment decisions, establish limitations for using AI in elections, and prohibit deep fakes.

WHAT'S IN THE UTAH AI ACT?

Utah's AI Act includes a number of key provisions.

Gen AI Transparency Disclosures

The Utah AI Act is focused on the use of "generative artificial intelligence," which is defined as an artificial system that:

* The authors, attorneys with Willkie Farr & Gallagher LLP, may be contacted at dalvarez@willkie.com, ljehl@willkie.com, bpollard@willkie.com, srohol@willkie.com and kprochaska@willkie.com, respectively.

(1) Is trained on data;

(2) Interacts with a person using text, audio, or visual communication; and

(3) Generates non-scripted outputs similar to outputs created by a human, with limited or no human oversight.[1]

The Utah AI Act requires that certain disclosures be made to individuals regarding their interactions with Gen AI, depending on the status of the entity. Specifically:

- When a business or person uses Gen AI to interact with an individual, the business or person is required to disclose that the individual is interacting with Gen AI only if the individual asks whether the interaction involves Gen AI.
- When Gen AI is utilized in the provision of services of "regulated occupations" (e.g., those that require a license or state certification, from accountants and certain financial advisors, to physicians, dentists, and nurses), a prominent mandatory disclosure must be clearly and conspicuously provided. Regulated occupation professionals must disclose either verbally (at the start of an exchange or conversation) or through an electronic message (before a written exchange) the use of Gen AI.
- Penalties for violations are up to $2,500 for each violation – if each interaction with a consumer is a potential violation, the total liability for a company's non-compliance may be significant. Utah's Division of Consumer Protection may impose administrative fines or bring an action in court. Courts may also impose the fine, issue an injunction, order disgorgement of any money received in violation of the Utah AI Act, or order payment of disgorged money to an injured person.

AI Learning Lab and Regulatory Mitigation

The Utah AI Act also establishes the Artificial Learning Laboratory Program (the Program), which is designed to analyze and research the risk, benefits, impacts, and policy implications of AI technologies. It also introduces the concept of "regulatory mitigation," which allows Program participants to develop and test AI technology while benefiting from limited liability that could arise from participation in the Program (e.g., a cure period before penalties may be assessed and reduced civil fines during the participation term).

Under the Program, to be eligible for regulatory mitigation, participants must meet certain requirements, including:

[1] S.B. 149 Artificial Intelligence Amendments, § 13-2-12(1)(a).

(1) Technical expertise to develop the proposed AI technology;

(2) Sufficient financial resources to meet testing obligations; and

(3) An effective plan to monitor identified risks from testing.

A regulatory mitigation agreement must specify:

(1) Limitations on scope of the use of a participant's AI technology, including the number and type of users and geographic limitations;

(2) The safeguards to be implemented; and

(3) Any regulatory mitigation granted to an applicant to the Program.

Dedicated Policy Office and Learning Laboratory

The Utah AI Act also mandates the formation of the Office of Artificial Intelligence Policy, which assumes responsibility for:

(1) The creation and administration of the Program;

(2) Consultation with stakeholders and businesses regarding regulatory proposals; and

(3) The establishment of rulemaking for participation, cybersecurity, data use, and consumer disclosures.

WHAT'S IN COLORADO'S AI ACT?

The Colorado AI Act is the first comprehensive state law in the U.S. governing AI. Its focus is high-risk AI systems, which are defined as "any artificial intelligence system that, when deployed, makes, or is, a substantial factor in making, a consequential decision."[2] This is a significantly broader scope than the Utah AI Act, and likely to implicate more business's uses of AI tools.

Obligations for Developers and Deployers of High-Risk AI Systems

A "developer" is defined as any person doing business in Colorado that develops or intentionally and substantially modifies an AI system. Developers of high-risk AI systems have a duty to avoid algorithmic discrimination, and there is a rebuttable presumption that a developer used reasonable care if the developer complied with the obligations imposed by the Colorado AI Act and any additional rules promulgated by the Colorado's Attorney General. Some specific obligations for developers include:

[2] Senate Bill 24-205 Concerning Consumer Protections in Interactions with Artificial Intelligence Systems, Colorado General Assembly, § 6-1-1701(4); A consequential decision means "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: (a) Education . . . ; (b) Employment . . . ; (c) A financial or lending service; (d) An essential government service; (e) Health-care services; (f) Housing, (g) Insurance, or (h) A legal service," id. at §6-1-1701(3).

- Providing to deployers of high-risk AI systems a statement describing the foreseeable uses and known harmful or inappropriate uses of the system, as well as a summary of the data used to train the system and documentation regarding mitigation measures and performance evaluations;
- Making publicly-available a summary of (a) its high-risk AI systems made available to deployers, and (b) how the developer manages risks of algorithmic discrimination; and
- Reporting to the Colorado Attorney General and known deployers of the high-risk AI system any known or reasonably foreseeable risks of algorithmic discrimination within 90 days after the discovery of any such risks through either ongoing self-testing or a credible report from a deployer.

The Colorado AI Act also requires deployers – defined as a person doing business in Colorado that deploys a high-risk artificial intelligence system – to use reasonable care to avoid algorithmic discrimination in a high-risk AI system. Similar to developers, there is a rebuttable presumption that a deployer has used reasonable care if the deployer complied with particular requirements in the bill and any rules enacted by the Colorado Attorney General. Some specific requirements of deployers of high-risk AI systems include:

- Implementing a risk management policy and program to govern the use of the high-risk AI system;
- Performing an annual impact assessment of the high-risk system and within ninety (90) days after any intentional and substantial modification to the system;
- Notifying consumers (prior to deployment) that a high-risk AI system will be used to make, or is a substantial factor in making, a consequential decision, and informing consumers of their rights, including rights under the Colorado Privacy Act; and
- Making publicly-available a statement that summarizes the types of high-risk AI systems that the deployer currently deploys, how the deployer manages any known or reasonably foreseeable risks of algorithmic discrimination that may arise from such systems, and the nature, source, and extent of the information collected and used by the deployer.

Disclosure of an AI Interaction

Developers and deployers of AI systems that intend to interact with consumers must disclose to the consumer that such interaction is taking place, unless it would be obvious for a reasonable person that the said interaction is with an AI system.

AI Systems and Consumer Rights

The Colorado AI Act provides consumers with the following rights in the event a high-risk AI system makes a consequential decision that is adverse to a consumer:

- *Explanation*. The consumer must be provided with a statement explaining the principal reason(s) for the consequential decision, which should include the degree in which the high-risk AI system contributed to the decision, the type of data processed in making the decision, and data sources involved in the decision.

- *Correction*. A consumer must be provided with an opportunity to correct any erroneous personal information used by the high-risk AI system to make a consequential decision.

- *Appeal*. The consumer must have an opportunity to appeal the decision for human review, but only to the extent that such review is technically feasible.

Compliance Deadline

The Colorado AI Act will take effect on February 1, 2026. It is unclear how much the substantive requirements may change between now and then: in signing the bill, Governor Polis noted some concerns with the legislation, and encouraged lawmakers and stakeholders to work together to amend the Colorado AI Act and to have discussions to protect "the development and expansion of new technologies in Colorado" and allow consumers to "fully access important AI-based products."[3]

WHAT ELSE IS COMING? A PREVIEW OF OTHER AI LEGISLATION AND POLICYMAKING

While the Utah and Colorado have led the way, other states are considering broad legislation that would potentially implicate all manner of AI use cases. In California, for example, there are AI-related efforts on both the legislative and regulatory fronts. Several AI bills related to transparency,[4] disclosure requirements for training data sets,[5] synthetic content,[6] and safety and security,[7] are quickly advancing in the state legislature. Likewise, in March 2024, the CPPA voted 3-2 in favor of advancing the eagerly awaited proposed regulations to address automated decision-making technology (ADMT). It is expected that the CPPA's formal rulemaking process regarding ADMT will likely begin in July 2024 and is anticipated to be finalized in March 2025.

[3] SB24/205 Signing Statement, Governor Jared Polis, State of Colorado, located at https://drive.google.com/file/d/1i2cA3IG93VViNbzXu9LPgbTrZGqhyRgM/view?pli=1.

[4] SB-942, "California AI Transparency Act," California State Senate, 2024.

[5] AB-2013, "Artificial Intelligence: training data transparency," California State Assembly, 2024.

[6] SB-970, "Artificial Intelligence Technology," California State Senate, 2024.

[7] SB-1047, "Safe and Secure Innovation for Frontier Artificial Intelligence Models Act," California State Senate, 2024.