SQUIRE PATTON BOGGS

All Eyes on AI

Colorado Governor Throws Down the Gauntlet on Artificial Intelligence (AI) Regulation After Colorado General Assembly Passes the Nation's First AI Law

May 22, 2024

The week starting May 13, 2024, was a busy one for AI regulation. The week started and ended with big news from Colorado: on Monday, Colorado's legislature passed "Concerning Consumer Protections In Interactions With Artificial Intelligence Systems" (SB 24-205) (**Colorado AI Law**) and, on Friday, Governor Jared Polis (D) signed the Colorado AI Law "with reservations" according to his letter to Colorado's legislature. Although the Colorado legislature is the first US lawmaker to pass general AI legislation, Colorado's Governor has expressly invited the US Congress to replace the Colorado AI Law with a national regulatory scheme before the Colorado AI Law's February 1, 2026, effective date.

That same week, on Tuesday, May 14, Senate Intelligence Committee Chairman Mark R. Warner (D-VA) asked companies who signed onto the AI Elections Accord for details about their efforts to combat use of AI for election interference. On Wednesday, May 15, the bipartisan Senate AI Working Group released a much-anticipated report on the findings from its nine "Insight Forums," outlining a proposed roadmap for federal AI policy (discussed below). And, on Thursday, May 16, the US Department of Labor released its "Artificial Intelligence and Worker Wellbeing: Principles for Developers and Employers."

Whether the US Congress can develop a federal AI regime that preempts the developing body of state and local AI laws still is an open question. In the meantime, Colorado has framed the discussion and will be the *de facto* standard if the US Congress fails to take the lead.

In the wake of the Colorado AI Law, Texas and other states are considering their own comprehensive AI legislation. Will there emerge a patchwork of both overlapping and differing state laws as we have seen with privacy legislation? Can regulation prevent material harm without stifling innovation?

Photo credit: "Tsunami of AI Legislation" created by Prof. Eric Goldman using Dali-E GPT4 by Open AI. His musings on the role and risks of regulation of AI are here.

Colorado AI Law

Despite bipartisan congressional support for AI legislation, state and local lawmakers are the first movers on AI lawmaking – like with consumer privacy for which state leadership produced 18 (and counting) state consumer privacy laws.

In the first six weeks of 2024, the Business Software Association reported that more than 400 AI-specific bills were introduced in US state legislatures. With legislative seasons wrapping up for the summer, most of these proposed laws were tabled, including Connecticut's Act Concerning Artificial Intelligence, which faced a veto threat from Governor Lamont (D). The Colorado AI Law was the exception. Colorado joins New York City, which passed a local law regulating certain uses of AI in the workplace last year, as an AI regulatory trailblazer in the US.

Q1. What organizations are regulated by the Colorado AI Law?

Legal and natural persons (Colo. Rev. Stat. § 6-1-102) that are operating in Colorado and develop and/or use "High-Risk Artificial Intelligence Systems" (***HAIS***, as defined in Q3 below) are subject to the Colorado AI Law.

Specifically, a "Deployer" uses a HAIS (Colo. Rev. Stat. § 6-1-1701(6)) and a "Developer" develops or "intentionally and substantially modifies" an "Artificial Intelligence System." Compliance obligations on both Deployers and Developers center on a HAIS (Colo. Rev. Stat. § 6-1-1701(7).)

For Developers, the phrase "intentional and substantial modification" is defined as a deliberate change to an Artificial Intelligence System that results in "any new or reasonably foreseeable risk of Algorithmic Discrimination" (Colo. Rev. Stat. § 6-1-1701(10).) (See Q 2 below for the definition of Algorithmic Discrimination.)

Not-for-profit organizations are not excluded, like the Colorado Privacy Act. Colorado state and local governments also appear to be in scope.

Q2. When are organizations required to comply with the Colorado AI Law?

Developers and Deployers have until February 1, 2026, to comply with the Colorado AI Law.

Q3. What types of AI technology are covered by the Colorado AI Law?

Compliance obligations apply to a HAIS. A HAIS is an "Artificial Intelligence System" that when deployed makes or is a "Substantial Factor" in making a "Consequential Decision."

- An Artificial Intelligence System is "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." (Colo. Rev. Stat. § 6-1-1701(2))
  - This definition is generally similar to the definition in the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0), which defines an AI System as "an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments." The NIST definition also adds that "AI systems are designed to operate with varying levels of autonomy." The similarity to the AI RMF is expected since, as described below, the AI RMF is used to help define a reasonableness standard for a risk management policy and to help a Developer, Deployer or other person in establishing an affirmative defense in an action brought under the Colorado AI Law.
- Substantial Factor means a factor that "(i) assists in making a Consequential Decision; (ii) is capable of altering the outcome of a Consequential Decision; and (iii) is generated by an Artificial Intelligence System" (Colo. Rev. Stat. § 6-1-1701(11).
- Consequential Decision means "a decision that has a material legal or similarly significant effect on the provision or denial to any Colorado resident (i.e., a Consumer) of, or the cost or terms of: (a) educational enrollment or an educational opportunity; (b) employment or an employment opportunity; (c) a financial or lending service; (d) an essential government service; (e) healthcare services; (f) housing; (g) insurance; or (h) a legal service." (Colo. Rev. Stat. § 6-1-1701(3).) The phrase "material legal or similarly significant effect" is not defined.

A HAIS does not include:

- An Artificial Intelligence System that is intended to perform narrow procedural tasks or to detect a decision-making pattern or deviation from a prior decision-making pattern and does not replace or influence prior human decisions without sufficient human review (Colo. Rev. Stat. § 6-1-1701(9).)
- 17 types of common technology, as long as the outputs are not a Substantial Factor in making a Consequential Decision. These technologies are fraud detection that does not use facial recognition, anti-malware, anti-virus, video games, calculators, cybersecurity, databases, data storage, firewalls, internet domain registration, internet website loading, networking, spam and robocall filtering, spell checking, spreadsheets, web caching, web hosting and natural language generative AI that is subject to an "acceptable use policy" prohibiting generation of content that is discriminatory or harmful. The terms "discriminatory" and "harmful" are not defined, although, as discussed below, the term Algorithmic Discrimination is defined.

Algorithmic Discrimination occurs when use of an Artificial Intelligence 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 the laws of this state or federal law" (Colo. Rev. Stat. § 6-1-1701(1).) Algorithmic Discrimination does not include testing to identify, mitigate or prevent discrimination or expanding an applicant, customer or participant pool to increase diversity or redress historical discrimination, among other exclusions (Colo. Rev. Stat. § 6-1-1701(1).) The Colorado AI Act imposes various obligations on Developers and Deployers to meet their express duty of each to avoid Algorithmic Discrimination.

Q4. Who are the "Consumers" protected by the Colorado AI Law?

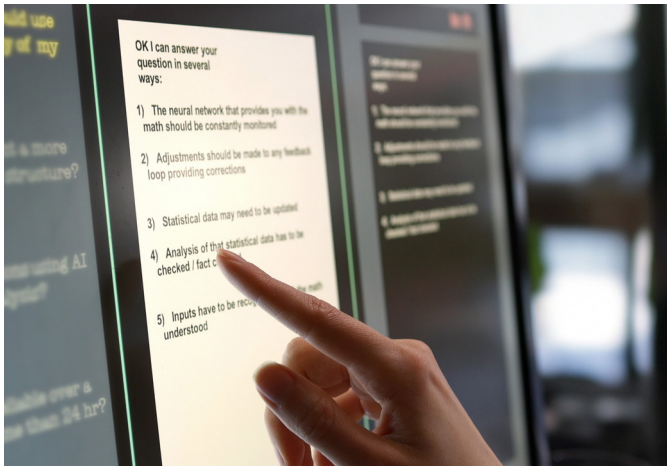
The Colorado AI Law is designed to protect "Consumers," defined as Colorado residents. As described below, Consumers have certain transparency rights and the right to correct personal data used to make certain decisions and, subject to narrow exceptions, the right of appeal to a human reviewer.

Q5. What compliance obligations apply to Developers?

The compliance obligations that apply to Developers are set forth in Colo. Rev. Stat. § 6-1-1702.

When developing a HAIS, the Developer must:

- **Duty of Care** – Exercise a duty of care to avoid Algorithmic Discrimination (which is defined in Q3 above) arising from "intended and contracted uses" (Colo. Rev. Stat. § 6-1-1702(1).)
- **Documentation** – Make certain documentation available for Deployers (Colo. Rev. Stat. § 6-1-1702(2)) which describes (*inter alia*):
  - High-level summary of training data used
  - The purpose and intended benefits and uses of the HAIS
  - Known and reasonably foreseeable limitations of the HAIS, including risks of Algorithmic Discrimination arising from intended uses
  - How risks were evaluated and mitigated before the HAIS was made available to Deployers
  - Data governance applicable to training data sets, including their suitability and biases
  - Mitigation measures for the HAIS' known and reasonably foreseeable risks arising from reasonably foreseeable deployment of the HAIS
  - When the HAIS is a Substantial Factor in a Consequential Decision, how the Deployer should use and not use the HAIS and when human monitoring is advisable
  - Other documentation "reasonably necessary to assist the Deployer in understanding the outputs and monitor [sic] the performance of the [HAIS] for risks of Algorithmic Discrimination."



- **Impact Assessment Information** – Make available information and documentation sufficient for a Deployer of the HAIS to conduct an impact assessment as required in Colo. Rev. Stat. § 6-1-1702(3).
- **Website Statement** – Publish on the Developer's website a statement that is clear and readily available and contains information about the types of HAIS that the Developer has developed and how the Developer manages known or reasonably foreseeable risks of Algorithmic Discrimination that arise during development and maintain the statement as accurate.
- **Attorney General Notification and Information Requests** – Notify the attorney general, and known Deployers, within 90 days after a discovery of, or credible report about, known or reasonably foreseeable risks of Algorithmic Discrimination arising from the HAIS' intended uses and respond to other information requests from the attorney general.

The Developer's disclosures and documentation requirements are limited by trade secret and confidential information protections as well as cybersecurity concerns (Colo. Rev. Stat. § 6-1-1702(6).)

Q6. What compliance obligations apply to Deployers?

The compliance obligations that apply to Deployers are set forth in Colo. Rev. Stat. § 6-1-1703 and focus on transparency and risk assessment and mitigation.

Specifically, when deploying a HAIS, the Deployer's obligations are:

- **Duty of Care** – Exercise a duty of care to protect Consumers from Algorithmic Discrimination.
- **Risk Management Policy and Program** – Implement a risk management policy and program for HAIS use that includes specific "principles, processes and personnel" used to identify, document and mitigate known or reasonably foreseeable risks of Algorithmic Discrimination over the HAIS' lifecycle.
  - The NIST AI RMF (see Q3) or equivalent risk management framework for AI that is nationally or internationally recognized or is designated and disseminated by the attorney general is the basis for considering the reasonableness of the Deployer's risk management policy and program.

- **Impact Assessment** – Complete an impact assessment for a deployed HAIS at least annually and within 90 days after any intentional and substantial modification to the HAIS (Colo. Rev. Stat. § 6-1-1703(3).) The impact assessment must meet specific content requirements including: a description of inputs and outputs; metrics used to evaluate performance and limitations; a description of transparency measures; and a plan for post-deployment monitoring.
- **Transparency Obligations** – A Deployer also has four main Consumer transparency obligations:

  i. **Pre-deployment Notice** – Prior to the deployment of a HAIS that makes or is a Substantial Factor in making a Consequential Decision, the Deployer must notify affected Consumers about the HAIS, including its purpose and the nature of the Consequential Decision; the contact information for the Deployer; how to access the Deployer's statement about its HAIS use and risk management (see iii. below); and how to access information about the Consumer's right to opt out of the processing of personal data concerning the Consumer for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the Consumer as required by § 6-1-1306 (1)(a)(I)(C) of the Colorado Privacy Act. (See also Q 10 below.)

  ii. **Adverse Consequential Decision Notice** – A direct notice to a Consumer who was the subject of an adverse Consequential Decision, including the reasons for the adverse Consequential Decision and type(s) of data processed in making the adverse Consequential Decision and the sources of that data, the Consumer's right to correct incorrect personal data used in the HAIS' Consequential Decision and the Consumer's right of appeal for the Consequential Decision (Colo. Rev. Stat. § 6-1-1703(4)(b).)

  iii. **Website Statement** – A clear and readily available website statement that is "periodically" updated about the Deployer's currently deployed HAIS and how the Deployer manages known or reasonably foreseeable risks of Algorithmic Discrimination; and "in detail", the nature, source and extent of the information collected and used by the Deployer.

  iv. **Generative AI Notice** – Notice to Consumers about the Deployer's Artificial Intelligence System (i.e., broader than a HAIS) with which the Consumer interacts unless the interaction with the Artificial Intelligence System "would be obvious to a reasonable person" (Colo. Rev. Stat. § 6-1-1704.)

A Deployer also has the obligation to notify the attorney general, within 90 days of discovery of Algorithmic Discrimination caused by the HAIS, the form and manner for which is to be prescribed in regulations (Colo. Rev. Stat. § 6-1-1703(7).)

A small business (50 or fewer FTEs) Deployer of a HAIS has narrower compliance requirements, e.g., no risk management program or impact assessments are required, as long as the small business Deployer's own data is not used to train the HAIS and the HAIS' continued learning is not based on the small business Deployer's data, the HAIS is used as the Developer intended and the small business Deployer makes available to Consumers the Developer's impact assessment (Colo. Rev. Stat. § 6-1-1702(6).)

Q7. Does the Colorado AI Law have exemptions?

The Colorado AI Law has exemptions for certain HAIS and for certain Developers and Deployers, in each case subject to certain conditions.

Specifically, the Colorado AI Law does not apply when a HAIS was "approved, authorized, certified, cleared, developed or granted by a federal agency", is "in compliance with standards established by a federal agency" or is for "conducting research to support an application for approval or certification from a federal agency" (Colo. Rev. Stat. § 6-1-1705(5)(a)-(b).) An Artificial Intelligence System acquired by or for the US federal government or any federal agency or department also is out of scope (Colo. Rev. Stat. § 6-1-1705(6).)

The Colorado AI Law also does not apply to a covered entity (as defined in the Health Insurance Portability and Accountability Act) providing healthcare recommendations that: "are generated by an artificial intelligence system; require a healthcare provider to take action to implement the recommendations; and are not considered to be high-risk" (Colo. Rev. Stat. § 6-1-1705(5)(d).) Insurers, banks and credit unions are deemed "in full compliance" (i.e., exempt) when they comply with rules related to AI issued by the relevant regulatory bodies (Colo. Rev. Stat. § 6-1-1705(7)(8).)

For all of these exemptions, the Developer or Deployer bears the burden of proving the exemptions apply to the AI system that was developed or deployed, as applicable.

Q8. How is the Colorado AI Law enforced?

Unlike Colorado's general consumer protection law (Colo. Rev. Stat. § 6-1-113), the Colorado AI law does not allow for a private right of action (Colo. Rev. Stat. § 6-1-1706.) The attorney general has exclusive authority to enforce the Colorado AI Law. A violation is an unfair trade practice under § 6-1-105(1)(hhhh) of Colorado's consumer protection law.

Rebuttable Presumptions – In an enforcement action, a Developer has a rebuttable presumption that the Developer used reasonable care in developing its HAIS to protect Consumers from any known or reasonably foreseeable risks of Algorithmic Discrimination arising from the "intended and contracted uses" of the HAIS if the Developer complied with the transparency and documentation duties described in Colo. Rev. Stat. § 6-1-1702. A Deployer has a rebuttable presumption that it used reasonable care in developing its HAIS to protect Consumers from any known or reasonably foreseeable risks of Algorithmic Discrimination when the Deployer complies with the risk management documentation, impact assessment and transparency requirements described in Colo. Rev. Stat. § 6-1-1703.

Affirmative Defense – A Developer, Deployer or "other person" covered by the Colorado AI Law has an affirmative defense to an enforcement action brought by the attorney general when (a) it cures the violation as a result of feedback that the Developer, Deployer or other person encourages Deployers or users to provide; adversarial testing or red teaming (as defined by NIST) or an "internal review process" and (b) complies with the NIST AI RMF (see Q3) or an equivalent risk management framework for AI that is nationally or internationally recognized or is designated and disseminated by the attorney general (Colo. Rev. Stat. § 6-1-1706(3).)

Remedies – In an enforcement action, the attorney general may seek injunctive relief, an assurance of discontinuance (essentially a pre-suit settlement), damages, civil penalties of up to US$20,000 per violation and "other or further relief as may be necessary to obtain compliance." Each impacted Consumer or transaction is a separate violation under Colorado law and, if the impacted Consumer is elderly, then the civil penalty maximum jumps to US$50,000 (*see* Colo. Rev. Stat. § 6-1-101 et seq.)

9.Does the Colorado AI Law provide for rulemaking?

Yes, the attorney general is given broad authority to promulgate regulations to implement and enforce the Colorado AI Law (Colo. Rev. Stat. § 6-1-1707.) Regulations are expected to address, for Developers, documentation and notice requirements, and for Deployers, requirements for notices to Consumers, for the risk management policy and program and for impact assessments, as well as the details about the requirements for the rebuttable presumption and affirmative defense described above.

10. How does the Colorado AI Law compare to automated decision-making and profiling under the Colorado Privacy Act?

The Colorado AI Law offers Consumers some transparency, correction and adverse decision appeal rights but is not limited to personal data. Rather, the Colorado AI Law focuses on management of AI risk, rather than protection of personal data. Nonetheless, reading the Colorado AI Law together with the Colorado Privacy Act (CPA) helps more fully explicate how Colorado intends to address AI.

The CPA – like the other state consumer privacy laws now in effect (except for Utah's consumer privacy law) – regulate "profiling" and automated decision-making, but only the CPA currently has rules detailing controller obligations and consumer rights. (California has published draft regulations, but not yet submitted them for public comment. More on California here.)

Under CPA, "profiling" means "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location or movements" [emphasis added]. Colorado residents have the right, subject to various exceptions, to object to profiling that is "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." The CPA's rules further provide that requests to opt-out of profiling in furtherance of decisions that produce legal or other similarly significant effects "based on Solely Automated Processing or Human Reviewed Automated Processing shall be honored." However, with respect to profiling using personal data in furtherance of decisions that produce legal or similarly significant effects concerning the Consumer, if material human involvement is involved with reaching the ultimate decision (i.e., the AI informs a human decision, but is not determinative), then the Consumer may request to opt-out but an organization can reject the request and inform the Consumer, or share a link to the information, as required by the Colorado Privacy Act Rule 9.04(C), including access to the meaningful logic involved in decision-making.

The CPA also requires very detailed risk assessments regarding profiling, which must occur at least annually or more often if a profiling practice is modified. Given the high likelihood that the inputs to a HAIS include personal data, the CPA's assessment requirements overlap with the Colorado AI Law's assessment requirements. Accordingly, combining the assessment requirements under these two Colorado laws is a necessary compliance step unless/until the attorney general's regulations under the Colorado AI Law harmonize these requirements. Assessments under the CPA are subject to inspection by the attorney general, as are impact assessments under the Colorado AI Law (Colo. Rev. Stat. § 6-1-1703(9).)

11. How does the Colorado AI Law compare to the EU AI Act?

While Colorado takes the first mover position among US law makers, the EU adopted comprehensive AI regulation, the Artificial Intelligence Act (EU AI Act), on March 13, 2024, following years of study and consideration. The Colorado AI Law is in part aligned with the EU AI Act. Both laws follow a risk-based approach and have similar obligations for transparency, active monitoring for potential bias, record keeping, risk management, cybersecurity requirements and human oversight obligations. The EU AI Act has, however, a broader scope, e.g., adopting a risk categorization system, prohibiting certain high-risk AI systems and regulating even limited risk AI systems, and is generally more proscriptive and proactive than the Colorado AI Law.

The EU AI Act includes deterrence sanctions, with potential fines of up to €35 million or 7% of the previous year's revenue for developing or deploying banned AI systems and of up to €15 million or 3% for breaches of the EU AI Act's obligations. Penalties up to €7.5 million or 1.5% for merely providing incorrect information are possible. Each EU member state must to appoint an AI authority to monitor compliance by both developers and operators/users of AI systems. While the Colorado AI Act gives the attorney general meaningful remedies, including substantial civil penalty authority, the potential penalties under the Colorado AI Law are not as potentially impactful as those under the EU AI Act. The Colorado AI Law does not set up a new AI authority as the EU AI Act calls for, but empowers the attorney general to promulgate regulations and enforce the Colorado AI Law and its regulations, similar to the role given the attorney general in the CPA to act as the state's data protection authority. The attorney general has issued very detailed rules under the CPA, which add substantial additional obligations on controllers beyond what is explicitly required by the CPA. The attorney general could do the same under the Colorado AI Act.

Bipartisan Senate AI Working Group's AI Report and Policy Roadmap

While the Colorado AI Law was waiting for the Colorado Governor's signature, the bipartisan Senate Artificial Intelligence (AI) Working Group released its 30-page policy roadmap titled "Driving US Innovation in Artificial Intelligence" (***AI Working Group Report***) on May 15, 2024.

(The AI Working Group is led by Senate Majority Leader Chuck Schumer (D-NY), Sen. Martin Heinrich (D-NM), Sen. Mike Rounds (R-SD), and Sen. Todd Young (R-IN). Sens. Young, Rounds and Heinrich are collectively known as Schumer's "AI sherpas.")

The AI Working Group Report was based on learnings from the series of Insight Forums (i.e., listening sessions) held during Fall 2023. It is intended to outline a path forward for federal AI legislative efforts. Leader Schumer told reporters that the AI Working Group plans to task Senate committees of jurisdiction with action on the recommendations in the AI Working Group Report. He also said that the Senate would move forward on individual bills, rather than waiting for a larger package to take shape, which he initially proposed would flow from his 2023 SAFE Innovation Framework.

Leader Schumer identified AI election interference as a top priority for the Senate, but he did not indicate the timing for any pending legislation. On the same day, Senator Klobuchar announced that three election protection bills advanced out of the Senate Rules Committee: Protect Elections from Deceptive AI Act, AI Transparency in Elections Act and Preparing Election Administrators for AI Act.

Meanwhile, in the House, Speaker of the House Mike Johnson (R-LA) and House Democratic Leader Hakeem Jeffries (D-NY) announced (in February 2024) the establishment of a bipartisan Task Force on AI (House AI Task Force) to explore how to ensure America continues to lead the world in AI innovation while considering guardrails that may be appropriate for safeguarding the nation against current and emerging threats. Notably, the House AI Task Force has yet to release a framework or roadmap for legislative priorities in that chamber. Nevertheless, several AI bills were introduced in the House during the first and second session of the 118th Congress.

With all eyes currently on the Senate, AI legislation could move in that chamber this year – whether as standalone legislation or attached to an advancing legislative vehicle, such as the annual National Defense Authorization Act. In his letter to Colorado's legislature, Governor Polis calls for federal legislation, noting that a patchwork of state laws could "tamper innovation and deter competition in an open market" and that "the important work of protecting consumers from discrimination and other unintended consequences of nascent AI technologies is better considered and applied by the federal government."

We also flag that a potential "lame duck" session of Congress, which begins after the November elections, is a wildcard session, during which bills could advance unexpectedly in both chambers of Congress. With a divided Congress, the bills with the greatest prospect of advancing this year are those that Leader Schumer and his AI sherpas sponsor in the Senate or that have bipartisan and bicameral support.

Themes and Takeaways

The Colorado AI Law is structured around a duty of care to ensure responsible AI by Design, with proactive risk management required from both Developers and Deployers. It imposes for the first time in US law a specific legal duty to assess and mitigate bias in inputs, outputs and impact of AI.

For Developers of Artificial Intelligence Systems that were built prior to its enactment, the Colorado AI Law has some potentially challenging retroactive effects, such as training data provenance documentation requirements. Many elements of the Colorado AI Law are left up to the attorney general's broad rulemaking authority, which also creates uncertainty for Developers.

The Colorado AI Law builds on the Colorado Privacy Act but is broader because it has fewer exemptions and is not limited to personal data processing. The Colorado AI Law also offers two new rights for Consumers (right to notice of adverse Consequential Decision and right to appeal the adverse Consequential Decision for human review), as well as an expanded right to correct personal data. A Deployer also must inform Consumers about their rights under the Colorado Privacy Act related to opting out of profiling and correction of personal data, but the Colorado AI Law does not itself offer an opt-out right.

At the macro-level, all levels of government are concerned about legislating responsible and beneficial AI development in a manner that addresses risks of harm, but without hampering useful technology innovation. Colorado has given itself and the nation more than 18 months to sort out how to most appropriately address this concern and invited the US Congress to take the lead in doing so. In the meantime, until the Colorado AI Law is effective on February 1, 2026, it is the de-facto national standard (subject to amendment or preemption.) Stakeholders and policymakers must consider the strengths and shortcomings of the Colorado AI Law's approach in the meantime.

Prior to its effectiveness, the Colorado AI Law, and the NIST AI RMF (which the Colorado AI Law enshrines as reasonable risk management) represent best practices for AI developers and users as they implement responsible AI policies and programs in advance of established legal standards. For more information on how to implement and maintain a Responsible AI by Design program, please contact the authors and see our prior guidance here.

Contacts

The authors are grateful to **Krista Setera**, Paralegal, for her contributions.

Alan Friel
Partner and Chair, Global Data Privacy, Cybersecurity and Digital Assets Practice, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Julia Jacobson
Partner, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com

Stacy Swanson
Public Policy Advisor, Washington DC
T +1 202 457 5627
E stacy.swanson@squirepb.com

Bartolome Martin
Partner, Madrid
T +34 91 426 4867
E bartolome.martin@squirepb.com

Kyle Dull
Senior Associate, New York and Miami
T +1 212 872 9867
E kyle.dull@squirepb.com

2023 Global Data Review Ranked "Elite" and top 20 law firm for data

Quick, pragmatic and business-savvy advice"

Global Data Review 2023

[The] team at SPB provides stellar work product, is efficient and is always on the cutting edge of the latest regulations"

Global Data Review 2023

They are very knowledgeable and able to provide feedback and services in an agile manner that is business friendly."

Global Data Review 2023

Privacy World Blog

Keeping you informed on the evolving law on data privacy, security and innovation.