U.S. LEGISLATION

US POLICY

The Colorado Artificial Intelligence Act

FPF U.S. Legislation Policy Brief

July 2024

Authored By: **Tatiana Rice**, Deputy Director, U.S. Legislation
Keir Lamont, Director, U.S. Legislation
Jordan Francis, Policy Counsel, U.S. Legislation

Executive Summary

This Policy Brief summarizes and analyzes key elements of the Colorado AI Act (CAIA), which was passed by the legislature on May 8, 2024 and signed by the Governor on May 17.[1] It further describes what the CAIA will do if enacted in its current form and identifies FPF's most significant observations about the law.[2]

The CAIA is the first United States law to comprehensively regulate the development and use of high-risk artificial intelligence systems, and will come into effect on February 1, 2026–preceding even the European Union AI Act and therefore potentially becoming the first effective comprehensive AI law in the world. Highlights of the CAIA and our observations include:

- **Broader Potential Scope of Regulated Entities:** Unlike state data privacy laws, which typically apply to covered entities that meet certain thresholds, the CAIA applies to any person or entity that is a developer or deployer of a high-risk AI system. Additionally, one section of the law applies to any entity offering or deploying any consumer-facing AI system.
- **Role-Specific Obligations:** The CAIA apportions role-specific obligations for deployers and developers, akin to controllers and processors under data privacy regimes. Deployers, who directly interact with individuals and ultimately control how the system is used, are required to maintain risk management programs, conduct impact assessments, and provide relevant consumer rights. Developers, on the other hand, must provide the information and documentation needed for deployers to fulfill their responsibilities.
- **Duty of Care to Mitigate Algorithmic Discrimination:** Developers and deployers are subject to a duty of care to protect consumers from algorithmic discrimination, which in practice, likely means that enforcers of the CAIA will assess developer and deployer actions using a proportionality test. The definition of "algorithmic discrimination" appears to cover both intentional discrimination and disparate impact.
- **Novel Consumer Rights:** In addition to typical consumer rights seen in comparable legislation, such as the right to pre-use notice, the CAIA provides consumers with particular rights if an adverse decision is made by a high-risk AI system. In that event, the deployer must provide a consumer a statement of reasons, the right to correct, and appeal for human review, if feasible.
- **Attorney General Authority:** Though the CAIA does not create a private right of action, it grants the Colorado Attorney General significant authority to enforce the law and implement necessary regulations.

[1] The Colorado AI Act was introduced by Senate Majority Leader Robert Rodriguez and co-sponsored by Senators Cutter, Michaelson Jenet, Priola, Winter, Fenberg and House Representatives Titone, Rutinel, and Duran. The bill closely follows the framework established in Connecticut Senate Bill 2 by Connecticut Senator Maroney.

[2] The CAIA may undergo revisions pursuant to Attorney General rulemaking (detailed in Sec. 8) and the legislative task force established in companion bill HB 1468.

This brief addresses the following elements of the CAIA:

1. Scope & Regulated Entities
2. Algorithmic Discrimination
3. Developer Obligations
4. Deployer Obligations
5. Consumer Rights
6. Other Disclosures
7. Exemptions
8. Enforcement and Defenses

1. Scope & Regulated Entities

Most of the CAIA regulates developers and deployers of "**high-risk artificial intelligence systems**" defined as "any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision." (Sec. (Sec. 6-1-1701(9(a)). In turn, the two operative terms in that description are defined as follows:

1. A "**consequential decision**" is any decision that has a material, legal, or similarly significant effect on the provision of denial to, or the cost or terms of the following categories: education, employment, financial or lending services, essential government services, healthcare services, housing, insurance, or legal services. (Sec. 6-1-1701(3)).
2. A "**substantial factor**" is a factor generated by an AI system that is used to assist in making, and is capable of altering the outcome of, a consequential decision (Sec. 6-1-1701(11)).

"High-risk artificial intelligence system" excludes AI systems intended to perform a narrow procedural task or detect decision-making patterns or deviations from prior decision-making patterns. (Sec. 6-1-1701(9)(b)). The following technologies are also excluded, so far as they are not used to make or be a substantial factor in making a consequential decision:

- Anti-fraud (non-facial recognition);
- Anti-malware, anti-virus, and firewall;
- Video games;
- Calculators;
- Cybersecurity;
- Databases and data storage;
- Internet domain registration, website loading, and networking;
- Spam and robocall- filtering
- Spell-checking;
- Spreadsheets;
- Web caching or web hosting;
- Interactive technologies that provide users information ("chatbots") **if such system is subject to an accepted use policy** that prohibits generating discriminatory or harmful content

Both developers and deployers of high-risk artificial intelligence systems ("high-risk AI systems") must conduct business in Colorado for the law to apply. While a deployer is simply defined as anyone that deploys a high-risk AI system, a developer includes anyone who develops an AI system, as well as anyone who "**intentionally and substantially modifies**" an AI system in a manner that results in any new foreseeable risk of algorithmic discrimination. (Secs. 6-1-1701(6), 6-1-1701(10)).

Observations:

- **No Covered Entity Thresholds:** Unlike state data privacy laws, which typically apply to covered entities that collect or sell a certain amount of data or meet a revenue threshold, the CAIA applies to any person or entity that is a developer or deployer of a high-risk AI system. Though there are limited exemptions for small deployers, Governor Polis noted particular concerns with the law's impact on the state's innovation economy and competition.
- **Detailed List of Excluded Technologies:** Critics might find it redundant for the CAIA to list technologies excluded from the law's scope since they ordinarily wouldn't make or substantially influence consequential decisions. However, the bill sponsor likely included the list to maximize clarity and gain stakeholder support, avoiding arguments about overbreadth, as seen with the California Privacy Protection Agency's draft regulations on "automated decisionmaking technology." Consequently, the CAIA's exclusions encompass all technologies excluded under the CPPA draft regulations, plus additional ones.
  - With the exclusion regarding chatbots, the basis for the exclusion itself–that there must be an accepted use policy–may be a way to incentivize ethical conduct without direct regulation.

2. Algorithmic Discrimination

A primary goal of the CAIA is to mitigate the risk of "**algorithmic discrimination**," defined as any condition in which the use of an AI 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 protected class, including, e.g., age, color, disability, ethnicity, national origin, race, religion, reproductive health, sex, or veteran status. (Sec. 6-1-1701(1)). Self-testing for bias, activities that support increased diversification, and acts conducted by a private club that are currently exempted under civil rights law do not constitute "algorithmic discrimination." (Sec. 6-1-1701(1)(b)).

Both developers and deployers are subject to a **duty of care,** meaning they must use "reasonable care" to protect consumers from "any **known or reasonably foreseeable risks of algorithmic discrimination** from the intended and contracted uses" of the high-risk AI system.

Developers and deployers maintain a rebuttable presumption of using reasonable care under this provision if they satisfy the obligations of the CAIA.

Observations:

- **Duty of Care Versus Prohibition:** Rather than include a prohibition against algorithmic discrimination, as seen in California AB 2930 (2024) or the District of Columbia's Stop Discrimination by Algorithm Act (SDAA) (2021), the CAIA imposes a "duty of care" with a "reasonability" standard. In practice, this likely means the CAIA does not impose strict liability. Instead, developers and deployers may be assessed using a proportionality test, considering factors, circumstances, and industry standards, to determine whether they exercised reasonable care to prevent algorithmic discrimination.
- **Interaction with Existing Civil Rights Law:** Although most agree that civil rights laws already apply to AI systems in theory, civil rights experts note that the law is far behind the technology, making the CAIA a step in the right direction. Given the law's intent, the CAIA will certainly interact with existing civil rights law, though it's unclear precisely how. As a result, the CAIA has drawn criticism from industry for creating uncertainty, and civil society advocates for potentially weakening or conflicting with existing rights. Some observations:
  - **Clarifying the Status Quo:** The law's definition of "algorithmic discrimination" as "unlawful differential treatment" may signal the bill sponsor's intent not to expand existing civil rights law, but provide clarity that existing law applies to the AI context as well.
  - **Disparate Impact:** The CAIA appears to cover both intentional discrimination and disparate impact, where seemingly neutral practices disproportionately affect one group of people with a protected characteristic more than another. In his signing statement, Governor Polis urged the legislature to reexamine the law to focus primarily on intentional discrimination. However, federal regulators, data scientists, and civil rights advocates argue that disparate impact is a necessary component of ensuring AI non-discrimination.

3. Developer Obligations

Beyond the duty of care, developers must adhere to several transparency requirements outlined in Section 6-1-1702. Compliance with these requirements enables developers to maintain a rebuttable presumption that they exercised reasonable care to mitigate algorithmic discrimination. These obligations include:

Disclosures to Deployers: Developers must make available to deployers and other developers of the high-risk AI system a "**general statement"** describing the reasonably foreseeable uses and known harmful or inappropriate uses" of the system and the following forms of"**documentation**":

1. **Information for Compliance:** Information necessary for the deployer to comply with their obligations under the law, including high-level summaries of the types of data used to train the system, known or reasonably foreseeable limitations of the system, the system purpose, and its intended benefits and uses (Sec. 6-1-1702 (2)(b));
2. **Evaluation & Mitigation:** Documentation describing how the system was evaluated for performance and mitigation of algorithmic discrimination, data governance measures concerning source and bias, intended outputs of the system, measures taken to mitigate known or reasonably foreseeable risks of algorithmic discrimination, and how the system should be used, not be used, and be monitored while in use (Sec. 6-1-1702 (2)(c));
3. **As Necessary:** Additional documentation reasonably necessary for a deployer to understand the systems' outputs and monitor its performance for risks of algorithmic discrimination (Sec. 6-1-1702 (2)(d));
4. **Facilitating Impact Assessments:** Information and documentation, "through artifacts such as model cards, dataset cards, or other impact assessments," necessary to complete an impact assessment, either by the deployer or a contracted third party (Sec. 6-1-1702 (3)).

Upon request by the Attorney General, a developer has ninety days to disclose the statement or documentation disclosed to deployers as described above (Sec. 6-1-1702 (7)).

Disclosures to the Public: Developers must make available on their website or in a public use case inventory—and update as necessary or within ninety days of an intentional and substantial modification—a statement summarizing (1) the types of high-risk AI systems it currently makes available to deployers or other developers; and (2) how the developer manages known or reasonably foreseeable risks of algorithmic discrimination (Sec. 6-1-1702 (4)).

Notification of Algorithmic Discrimination: Within ninety days of discovering, either through their own testing and analysis or via a credible report from a deployer, that their high-risk AI system has caused or is reasonably likely to have caused algorithmic discrimination, a developer must disclose those known or reasonably foreseeable risks to the attorney general and *all known deployers* (Sec. 6-1-1702 (5)).

Observations:

- **Comparison with Controller/Processor Distinction:** Similar to how "processors" are treated under many data privacy regimes, the CAIA places fewer affirmative obligations on the "developer" due to their lack of interaction directly with consumers or ability to ultimately control how the system is used. However, a deployer may also be subject to developer duties and liability if they significantly modify a system, creating a new or reasonably foreseeable risk of algorithmic discrimination.
- **Notifying Credible Reports of Discrimination:** The CAIA goes beyond what would have been required under Connecticut Senate Bill 2, on which this law was modeled, by requiring that developers alert the Attorney General if they identify or otherwise receive

from a deployer a ***credible report*** that a deployed high-risk AI system has caused algorithmic discrimination.

- This requirement has faced significant pushback from industry, who argue that developers are ill-equipped to discover algorithmic discrimination by their deployers. Similarly, it may be challenging to distinguish between a system exhibiting bias against a single individual and reporting each of those cases versus reporting an illegal pattern of disparate impact against a protected class.
- As detailed in the enforcement section, however, the developer maintains an affirmative defense against Attorney General enforcement arising from such discrimination if they cure any violation of the Act and are otherwise compliant with a recognized risk management framework.

4. Deployer Obligations

Deployers must comply with the requirements outlined in Section 6-1-1703, which mandate transparency, the establishment of internal AI governance practices and policies, and the provision and response to consumer rights. Like developers, deployers must adhere to a duty of care regarding algorithmic discrimination. They can benefit from a rebuttable presumption of having acted with care if they comply with the requirements of Section 6-1-1703 and any additional regulations issued by the Attorney General. These requirements include—

Risk Management Policy & Program: Deployers must implement a risk management policy and program to govern their deployment of a high-risk AI system (Sec. 6-1-1703 (2)). The risk management policy and program must (1) specify the principles, processes, and personnel used to identify and mitigate algorithmic discrimination; (2) be an iterative process that is reviewed and updated regularly; and (3) be reasonable, considering factors such as how the framework compares to the latest version of the "Artificial Intelligence Risk Management Framework" (AI RMF) published by the National Institute of Standards and Technology (NIST) and the size and complexity of the deployer (Sec. 6-1-1703 (2)(a)). One risk management policy and program can cover multiple high-risk AI systems deployed by the deployer (Sec. 6-1-1703 (2)(b)).

Impact Assessments: Annually, and within ninety days after a substantial and intentional modification to a high-risk AI system, a deployer, or a third party contracted to the deployer, must conduct an impact assessment (Sec. 6-1-1703 (3)(a)). As detailed in Sec. 6-1-1703 (3)(b), impact assessments must include, to "the extent reasonably known by or available to the deployer,"—

1. **Purpose:** A statement disclosing the system's purpose, intended use cases, deployment context, and benefits (and, if after an intentional and substantial modification, a statement disclosing the extent to which the [AI system] was used in a manner that was consistent with, or varied from, the developer's intended uses);
2. **Risk:** Analysis of whether there are known or reasonably foreseeable risks of algorithmic discrimination and, if so, the nature of those risks and mitigation steps taken;

3. **Data:** A description of categories of data processed as inputs and outputs produced by the system; and an overview of categories of data used to customize the system, if applicable;
4. **Testing:** Metrics used to evaluate the system's performance and known limitations;
5. **Transparency:** A description of transparency measures taken including those to disclose to an individual that the system is in use when it is in use; and
6. **Monitoring:** Description of post-deployment monitoring and user safeguards, such as the deployer's "oversight, use, and learning process" to address issues arising from deployment

One impact assessment may cover "a comparable set" of deployed systems, and an assessment completed for complying with another law or regulation can satisfy the requirements of the CAIA if that other assessment "is reasonably similar in scope and effect" to the one required under the CAIA (Sec. 6-1-1703 (3)(d) & (e)). Impact assessments, and all records concerning each impact assessment, shall be retained for at least three years after the final deployment of the system (Sec. 6-1-1703 (3)(f)).

Disclosures to the Public: Deployers must make available on their websites, and periodically update, a statement summarizing the types of high-risk AI systems currently deployed, how known or reasonably foreseeable risks of algorithmic discrimination arising from deployment are being managed, and, "[i]n detail, the nature, source, and extent of the information collected and used by the deployer" (Sec. 6-1-1703(5)).

Review and Notification of Algorithmic Discrimination: Annually, deployers, or third parties contracted by deployers, must review the deployment of the system to ensure that it is not causing algorithmic discrimination (Sec. 6-1-1703 (3)(g)). If a deployer learns, post-deployment, that a system has caused algorithmic discrimination then the deployer must send to the attorney general, without unreasonable delay and within ninety days of the discovery, notice of the discovery (Sec. 6-1-1703 (7)).

Observations:

- **The Leading Role of the Colorado Attorney General in AI Governance:** One of the discretionary rulemaking powers of the Colorado Attorney General is the authority to determine which AI risk management frameworks are suitable for compliance under the CAIA. Consequently, the Colorado AG may be poised to play a leading national role in setting AI governance standards.
- **Flexible Metrics to Mitigate Discrimination:** The CAIA mandates that deployers mitigate algorithmic discrimination and annually assess their systems for such issues, but the law does not specify explicit testing or auditing requirements. In contrast, legislation like New York City Local Law 144, which mandates specific auditing practices, has faced criticism for imposing standards that are either undeveloped or use

inappropriate metrics. The CAIA avoids this by allowing deployers the flexibility to choose how to measure and test for bias, as long as these assessments are conducted and documented. However, civil society advocates argue that this flexibility may give entities too much leeway to declare their systems non-discriminatory.

5. Consumer Rights

Deployers owe certain obligations to individuals. No later than the time that a deployer uses a high-risk AI system to make a consequential decision, a deployer must **notify** individuals about the use of the system and provide a **statement** that discloses (1) the purpose of the system and nature of its consequential decision, (2) contact information for the deployer, (3) a plain language description of the system, (4) instructions for how to access the deployer's website disclosure, and (5) where applicable, inform individuals of their Colorado Privacy Act right to opt-out of profiling in furtherance of decisions with legal or similar significant effects. (Sec. 6-1-1703(4)(a)).

Where a deployer has used a high-risk artificial intelligence system to reach a consequential decision that is **adverse** to a person, the deployer is required to provide that person with an additional statement disclosing the "principal reason or reasons" for the decision including: (1) the degree to which and manner in which the system contributed to the decision, (2) the type of data processed by the system, and (3) the source or sources of the data. (Sec. 6-1-1703(4)(b)). In these circumstances, a deployer must also offer the person with (1) an opportunity to **correct** any inaccurate personal data the system processed for the decision and (2) an opportunity to **appeal** the decision that, where technically feasible and in the best interest of the person, allow for human review of the decision. ((6-1-1703(4)(b)(I) & (II)).

Observations:

- **Building upon Existing Privacy Law:** Broad-based data privacy rules are commonly regarded as a necessary first step for tackling the risks posed by high-risk AI systems. The CAIA implicitly builds upon the Colorado Privacy Act of 2022 ("CPA") which establishes rights and data controller obligations for the use of personal information. Notably, Senate Majority Leader Rodriguez was a primary sponsor of both laws. In this section, the CAIA directly points to the CPA's existing right to opt-out of profiling which presently exists in approximately 15 state 'comprehensive' privacy laws.
- **Contemporaneous Notice:** The CAIA requirement to provide individuals with notice "no later than the time" that a high-risk AI system is deployed to make a consequential decision is comparable to California Privacy Protection Agency's draft ADMT regulations which would require a "pre-use" notice to be provided to a consumer before processing the consumer's personal information using automated decisionmaking technology. The requirements for notices under CPPA's draft regulations are more prescriptive than the CAIA's disclosure requirements.

- **Alignment with Minnesota?** Minnesota's recently enacted comprehensive privacy law contains a unique right to contest the result of significant profiling decisions (not just opt-out of such decisions) that resembles the CAIA. This law grants individuals the right to be informed about actions they could take to secure a different decision, review the personal data used in profiling, correct inaccurate data, and have the profiling decision reevaluated. While Minnesota's law does not explicitly provide a right to human review, similar consumer rights to appeal the outcomes of significant automated decisions could become a standard feature in both AI and privacy-focused legislation.
- **Technical Feasibility:** The CAIA provides two exceptions to the right to human review of a high-risk AI system's adverse consequential decision. First, human review should be "technically feasible," and second, such review should be "in the best interest of the consumer" (noting that in some cases delay might pose a risk to life or safety). Stakeholders may seek clarification of both terms through Attorney General rulemaking. The concept of "technical feasibility" was first included in the CA AB 331 (2023), though was focused on requests to be subject to an alternative selection process.

6. Other Disclosures

Upon request by the Attorney General, a developer, deployer, or a third party contracted by the deployer has ninety days to provide the role-specific documentation required by the CAIA. The Attorney General may then evaluate these documents for compliance with the CAIA (Sec. 6-1-1702(7), 6-1-1703(9)). However, the Act's reporting and transparency requirements will not require a developer or deployer to disclose a **trade secret** or information protected from disclosure by state or federal law. (Sec. 6-1-1702(6), 6-1-1703(8)). To the extent that a deployer withholds information under this (or another) exception, they must notify a consumer and provide a basis for the withholding. Developers have an additional exemption from disclosing information that would create a **security risk**. (Sec. 6-1-1702(6)). The CAIA also provides that both developer and deplayer records disclosed to the Attorney General are exempt from disclosure under the Colorado Open Records Act and that such disclosures do not constitute a waiver of attorney-client privilege. (Sec. 6-1-1702(7) & 6-1-1703(9)).

Additionally, **any entity** that deploys, offers, or makes available **an artificial intelligence system** intended to interact with consumers must disclose this to the consumer, unless it would be "obvious to a reasonable person" that they are interacting with an AI system. (Sec. 6-1-704).

Observations:

- **Broader than Comparable Laws:** This provision applies not only to developers and deployers but to any entity using any type of consumer-facing AI system. The obligation to disclose to individuals that they are interacting with an AI system is broader than Utah SB 149 (2024), which requires such disclosure only for generative AI systems, and a 2019 California law that prohibits using bots to interact with people online with the intent to mislead them, unless the bot's nature is disclosed.

7. Exemptions

The CAIA includes a number of specific and general carve-outs from its provisions, some of which will be familiar to stakeholders with experience in state privacy law and some that are novel.

Small Business Exemption: The CAIA contains a limited **small business exception** available only to certain deployers. Deployers that use a high-risk artificial intelligence system that employ fewer than fifty full-time employees and do not train the system with their own data are exempted from risk management program, impact assessment, and public disclosure obligations. (Sec. 6-1-1703(6)).

Entity-Based Exemptions: The CAIA contains several entity-based exemptions, including for: (1) **HIPAA-regulated 'covered entities'** in providing health care recommendations that are not considered to be high risk; (2) **insurers** regulated by existing Colorado law on algorithms and predictive models; and (3) **financial institutions** subject to substantially equivalent or more stringent rules that apply to the use of high-risk artificial intelligence systems. (Sec. 6-1-1705(5), (7), (8)).

Approved Technology Exemptions: The CAIA also provides exemptions for developers or deployers of a high-risk AI system that have been otherwise approved, certified, or cleared by a federal agency, such as the Food and Drug Administration (FDA) or is otherwise in compliance with standards established by a federal agency so long as the standards are substantially equivalent or more stringent than those contained in the CAIA.

Purpose-Based Exceptions: Finally, the CAIA contains several purposes-based exceptions that largely correspond to exceptions to the Colorado Privacy Act. These exceptions provide that CAIA shall not restrict a the ability of a developer or deployer to comply with existing laws, legal investigations, or cooperate with law enforcement; take action concerning legal claims; take immediate steps to protect life or physical safety; protect against security incidents or other illegal activity (*except through facial recognition technology*); engage in public interest research; effectual product recalls; identify and repair technical errors. Unlike the Colorado Privacy Act, the CAIA contains an exception for pre-deployment research, and testing and development activities, echoing some exceptions found in the European Union AI Act. (Sec. 6-1-1705(1)-(4)).

Observations:

- **Trade Secrets Controversy:** While a “trade secret” exception is a common element across state privacy laws, including this provision in the CAIA generated significant substantial civil society opposition as a potential loophole.
- **Small Business Carveout:** Unlike privacy laws, which typically base small business exceptions on annual revenue or data processing thresholds, the CAIA’s threshold is based on the number of employees. While business size may not directly reflect the complexity or risk profile of an AI system, Connecticut Senator Maroney noted during the Senate hearing on SB 2, which the CAIA was modeled after, that this limited exemption responds to concerns from small businesses with limited resources, often using “off-the-shelf” AI products like hiring tools.
    - The reasoning behind the CAIA small business exemption differs from the approach taken by the Federal Trade Commission (FTC). Last year, the FTC initiated an enforcement action against Rite-Aid for employing "off-the-shelf" AI systems without adequate testing or monitoring.
    - An alternative model is under consideration with California AB 2930 which would exclude deployers with fewer than 25 employees that use automated decision tools that impact fewer than 1,000 people per year from the requirement to conduct impact assessments.
- **Application of HIPAA-Covered Entity Exception:** The CAIA provides a carveout for HIPAA-regulated entities using an AI system for healthcare decisions, provided the healthcare provider implements the recommendation and it's not deemed high risk. Similar to the exclusion for chatbots in the definition of "high-risk artificial intelligence system," this exception may encourage keeping a "doctor in the loop" without direct regulation. However, it's unclear if the term "high risk" in this exemption aligns with the CAIA's definition of a "high-risk artificial intelligence system," which involves systems substantially influencing consequential decisions in healthcare services or another category of high-risk healthcare recommendations.

8. Enforcement and Defenses

The Attorney General has sole authority to enforce the CAIA (Sec. 6-1-1706(1)). There is no basis for a private right of action (Sec. 6-1-1706(6)).

If an enforcement action is brought by the Attorney General, a developer, deployer, or other person may assert an **affirmative defense** if they (1) discover and cure the violation based on feedback, adversarial testing, or an internal review process; and (2) are compliant with the NIST AI RMF, another recognized national or international risk management framework, or any other risk management framework designated by the Attorney General (Sec. 6-1-1706(3). The developer, deployer, or other person who is subject to the enforcement action bears the burden of demonstrating the necessary elements of the affirmative defense (Sec. 6-1-1706(4)).

In addition to enforcement authority, the Attorney General has permissive rulemaking authority, as necessary for implementing and enforcing the CAIA, including:

- Documentation and requirements for developers;
- The contents of and requirements for the notices and disclosures by developers, deployers, and other persons offering a consumer-facing AI system;
- The content and requirements of the deployer's risk management policy and program;
- The content and requirements of the deployer's impact assessments;
- The requirements of the rebuttable presumptions; and
- The requirements for the affirmative defense and the process by which the Attorney General will recognize other risk management frameworks.

Observations:

- **Interoperability:** To avoid duplicative AI governance efforts, the CAIA includes mechanisms to facilitate interoperability with other regimes. These include allowing the use of impact assessments conducted under other laws to meet the CAIA's requirements and fulfilling the NIST AI RMF to satisfy the CAIA's risk management requirements or as a defense against enforcement actions.
- **Questions Around Enforcing Against Algorithmic Discrimination:** In the event of demonstrable discrimination arising from the use of an AI system, many questions remain about how such claims would be enforced: *would the Colorado Attorney General be able to bring two separate discrimination claims, given that they would be identical claims for the same conduct, raising potential double jeopardy concerns? Though there is no private right of action, can an individual use information disclosed under this law as a basis to exercise their existing civil rights? Conversely, if an action is brought against an entity for algorithmic discrimination under existing civil rights law, could the defendant utilize information or standards compliance under the CAIA as a defense?*

  Unless clarified through amendments by the task force next legislative session or Attorney General rulemaking, many of these questions might only be addressed through litigation.

Did we miss anything? Contact Tatiana Rice, Deputy Director for U.S. Legislation at trice@fpf.org, or email to inquire about joining the FPF U.S. Legislation Working Group.

Disclaimer: This policy brief is for informational purposes only and should not be used as legal advice.