FUTURE OF PRIVACY FORUM

Overview of Senate Bill 24-205 and U.S. State AI Legislation

Colorado AI Task Force

September 16, 2024

Future of Privacy Forum

The Supporters

200+	40+	20+	5
Companies	Leading Academics	Advocates and Civil Society	Foundations

The Mission

Privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.
Developing privacy protections, ethical norms, and workable business practices.

Tatiana Rice
Deputy Director, U.S. Legislation

Agenda

I. **Overview of Substantive Provisions**
   - A. Scope and Regulated Entities
   - B. Duty of Care: Algorithmic Discrimination
   - C. Developer Obligations
   - D. Deployer Obligations
   - E. Consumer Rights
   - F. Other Requirements

II. **Enforcement & Attorney General Authority**
   - A. Exemptions, Defenses, & Safe Harbors
   - B. Attorney General Rulemaking

III. **FPF Report on U.S. State AI Legislative Landscape**

IV. **Q&A**

FUTURE OF PRIVACY FORUM

SB 24-205: Scope and Regulated Entities

Developers and **Deployers** (doing business in Colorado) of "**High-Risk AI Systems**"

1. **"High Risk AI System"**
   a. *Any **artificial intelligence system**;*
   b. *That when deployed, makes, or is a **substantial factor** in making;*
   c. *A **consequential decision**. (Sec. 6-1-1701(9(a)).*

2. **Regulated Entities**
   a. "Developer"
   b. "Deployer"

3. **Carve-Outs or Exceptions**

SB 24-205: Scope and Regulated Entities

Types of Technologies: "High Risk AI System"

"High Risk AI System"

1. *Any **artificial intelligence system**;*
2. *That when deployed, makes, or is a **substantial factor** in making;*
3. *A **consequential decision**. (Sec. 6-1-1701(9(a)).*

"Artificial Intelligence"

"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." (Sec. 6-1-1701(3)).

SB 24-205: Scope and Regulated Entities

Types of Technologies: "High Risk AI System"

"High Risk AI System"

1. *Any **artificial intelligence system**;*
2. *That when deployed, makes, or is a **substantial factor** in making;*
3. *A **consequential decision**. (Sec. 6-1-1701(9(a)).*

"Consequential Decision": *Any decision that:*

1. *Has a **material, legal or similarly significant effect**;*
2. *On the **provision or denial** to any consumer of, or the cost or terms of:*
3. *Areas: (A) Education; (B) Employment; (C) Financial or lending services; (D) Essential government services; (E) Healthcare service; (F) Housing, (G) Insurance, or (H) Legal services. (Sec. 6-1-1701(3)).*

SB 24-205: Scope and Regulated Entities

Types of Technologies: "High Risk AI System"

"High Risk AI System"

1. *Any **artificial intelligence system**;*
2. *That when deployed, makes, or is a **substantial factor** in making;*
3. *A **consequential decision**. (Sec. 6-1-1701(9(a)).*

"Substantial Factor": *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)).*

Carve-Outs and Exclusions: Technology-Specific

"**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**: (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
  - 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

Regulated Entities: Developers and Deployers

Deployer: A Person Doing Business In This State That Deploys A High-Risk Artificial Intelligence System.

Developer: A Person Doing Business In This State That **Develops** Or **Intentionally And Substantially Modifies** An Artificial Intelligence System.

- "**Intentionally and Substantially Modifies:**" "A deliberate change…that results in any **new** reasonably **foreseeable risk of algorithmic discrimination**."
- Does not include a change if:
  - (i) the high-risk AI system continues to learn after the high-risk AI system is: (a) offered, sold, leased, licensed, given, or otherwise made available to a deployer; or (b) deployed;
  - (ii) the change is made…as a result of any learning described in subsection (10)(b)(i) of this section;
  - (iii) the change was predetermined by the deployer, or a third party contracted by the deployer, when the deployer or third party completed an initial impact assessment of such high-risk artificial intelligence system…; and
  - (iv) the change is included in technical documentation for the high-risk artificial intelligence system.

SB 24-205: Scope and Regulated Entities

Carve-Outs and Exclusions: Technology-Specific

Entity-Based Exemptions: (Sec. 6-1-1705)

- **HIPAA-regulated 'covered entities'** in providing health care recommendations that are not considered to be high risk;
- **Insurers** regulated by existing Colorado law on algorithms and predictive models;
- **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 Exemption: High-risk AI systems 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 Act.

Duty of Care: Algorithmic Discrimination

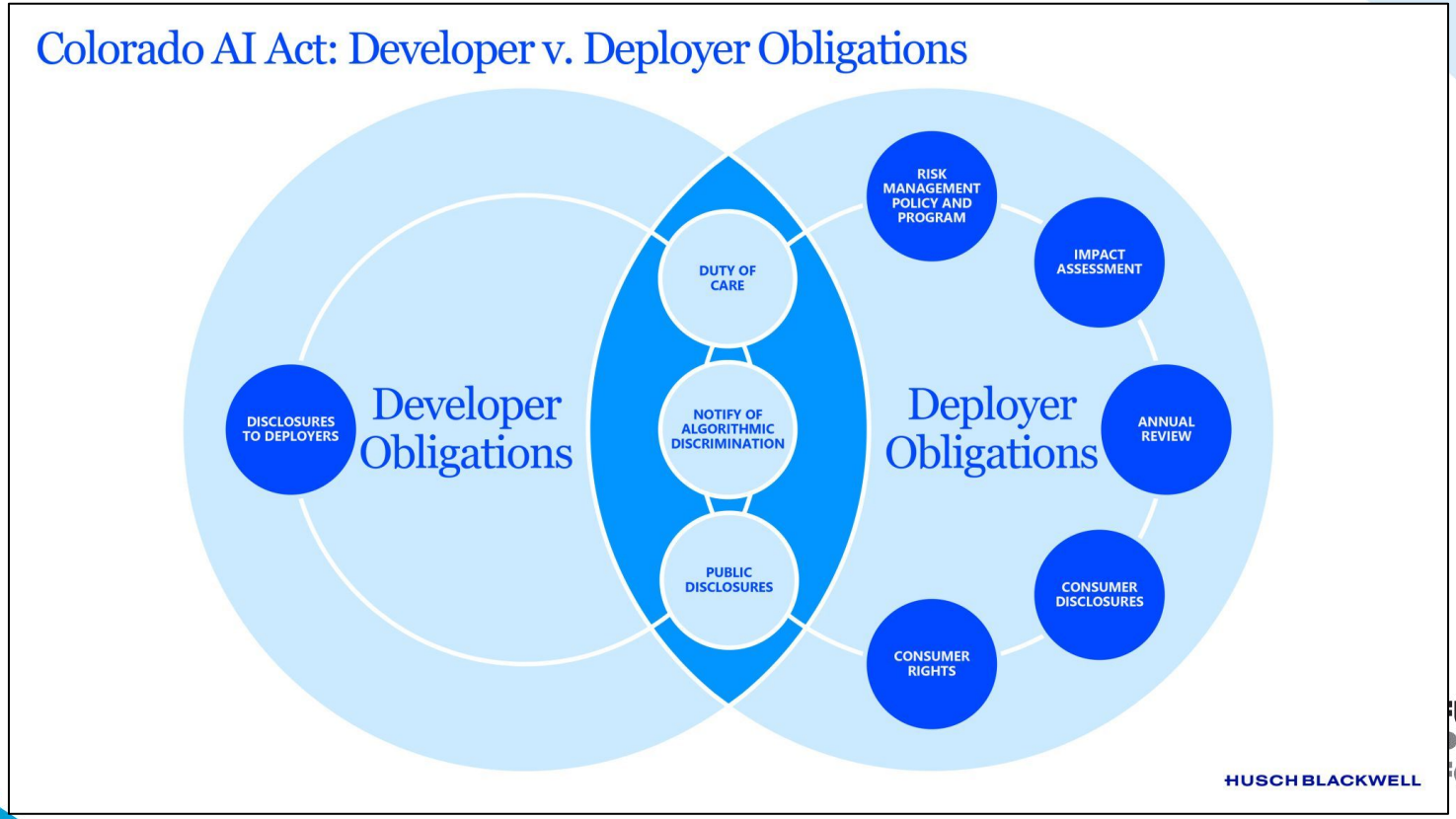
Algorithmic Discrimination: Any condition where the use of an AI system **results in unlawful differential treatment or impact** that disfavors an individual or group of individuals based on their protected class. (Sec. 6-1-1701(1)(a)).

- **EXCLUDES**: self-testing to mitigate or prevent discrimination or otherwise ensure compliance with state or federal law, expanding customer or applicant pool, private clubs.

Duty to Avoid Algorithmic Discrimination: Developers and Deployers shall use **reasonable care** to protect consumers from any **known or reasonably foreseeable** risk of algorithmic discrimination arising from the **intended and contracted use** 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 Act.

Developer and Deployer Obligations



SB 24-205: Developer Obligations

Disclosures to Deployer: 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":

- **Information for Deployer Compliance:** 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));
- **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));
- **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));
- **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)).

SB 24-205: Developer Obligations

- **Publicly Available Statement:** Maintain a publicly available summary of high-risk systems made available to deployers and risk management for algorithmic discrimination. (Sec. 6-1-1702(4)).

- **Available Documentation:** 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)).

- **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)).

SB 24-205: Deployer Obligations

- **Risk Management Policy:** Maintain a risk management policy that governs high-risk AI use, which specifies **processes and personnel** used to identify and mitigate algorithmic discrimination. (Sec. 6-1-1703(2)). Must be reasonable considering: NIST AI RMF, size of deployer, nature of system, sensitivity of data.

- **Impact Assessment:** Annually conduct (and upon each intentional and substantial modification) an impact assessment that details the purpose, intended use, risk of algorithmic discrimination, steps to mitigate such risks, description of data used and produced, performance, transparency measures, and post-deployment monitoring. Impact assessments must be retained for at least three years. (Sec. 6-1-1703(3)(a)-(b)).
    - ***Interoperability:*** An impact assessment conducted to comply with another relevant law or regulation is sufficient. (Sec. Sec. 6-1-1703(3)(e)).

SB 24-205: Deployer Obligations

- **Pre-Deployment Statement of Use:** Provide consumers subject to a high-risk system with a statement disclosing information about the high-risk AI system in use, including purpose, nature of the consequential decision, description of how the system assesses information to reach a decision, and sources of personal data processed, among other details. (Sec. 6-1-1703(4)(a)).

- **Publicly Available Statement:** Must make a statement regarding the use of a high-risk AI system available for public inspection. (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 that a system has caused algorithmic discrimination then 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)).

SB 24-205: Consumer Rights

- **Right to Pre-Use Notice:** Must be informed of any high-risk AI system used to make, or be a substantial factor in making, a consequential decision about the consumer, and a statement disclosing the purpose and nature of the system. (Sec. 6-1-1703(4)(a)).
- **Right to Exercise Data Privacy Rights:** Must be informed of the right to opt-out of profiling in furtherance of solely automated decisions, under the Colorado Privacy Act, and have the means to exercise those rights, if the deployer is a controller under the CPA. (Sec. Sec. 6-1-1703(4)(a)(III)).

If an adverse decision is made:

- **Right to Explanation:** The consumer must be provided a statement explaining the **principal reason** for the decision, the degree in which the high-risk AI system contributed to the decision, the type of data used in the decision, and the data source.
- **Right to Correct:** The consumer must be provided the opportunity to correct any inaccurate personal data used by the high-risk AI system in the decision.
- **Right to Appeal:** The consumer must be provided an opportunity to appeal that decision for human review, if technically feasible.

SB 24-205: General AI Disclosure

Any person or entity that deploys an artificial intelligence system intended to interact with consumers must disclose to the consumer that they are engaging with an AI system. (Sec. 6-1-1704).

SB 24-205: Enforcement and Attorney General Authority

The Attorney General shall have the sole exclusive authority to enforce.

Rulemaking: The Attorney General may promulgate rules to implement and enforce this Act, including requirements regarding:

- Developer documentation;
- Notice;
- Risk management;
- Impact assessment;
- Rebuttable presumptions; and
- Affirmative defenses, including other risk management frameworks that may be acknowledged for compliance.

SB 24-205: Enforcement Defenses and Safe Harbors

- **Small Business:** If a small business deployer (employing 50 or fewer full-time employees) meets certain requirements, they do not need to maintain a risk management program, conduct an impact assessment, or create a public statement. They are still subject to a duty of care and must provide the relevant consumer notices and rights. (Sec. 6-1-1703(6)).

- **Affirmative Defense:** If a developer or deployer (1) discovers and cures a violation through internal testing or red-teaming, and (2) otherwise complies with the NIST AI RMF or another nationally or internationally recognized risk management framework (Sec. 6-1-1706(3)).

FPF Report on U.S. State AI Legislative Landscape

Methodology

~33
States That Introduced Relevant AI Bills

~112
Relevant State AI Bills

17
Enacted AI Bills

*The Report also incorporates insights from **civil society groups, businesses, and technical experts,** whose diverse perspectives have been crucial in shaping a comprehensive examination of the nuances and challenges in advancing AI regulations.*

This report focuses on a handful of notable bills and laws at the state level, the majority of which were introduced in the 2024 legislative session. The most cited bills in this report are featured in table below,

Jurisdiction	Bill, Law, or Framework	Category
Colorado	SB 24-205 (Colorado AI Act) (enacted) **FPF Resource:** Policy Brief	Governance of AI in Consequential Decisions
California	AB 2930 (Automated Decision Systems) (proposed) (July 3, 2024)	Governance of AI in Consequential Decisions
Connecticut	SB 2 (proposed) (Apr. 24, 2024) **FPF Resource:** Blog Post	Governance of AI in Consequential Decisions
Virginia	HB 747 (proposed) (Feb. 5, 2024)	Governance of AI in Consequential Decisions
Vermont	H 710 (proposed) (Jan. 9, 2024)	Governance of AI in Consequential Decisions
Washington	HB 1951 (proposed) (Jan. 19, 2024)	Governance of AI in Consequential Decisions
Illinois	HB 3773 (enacted) (Aug. 9, 2024)	Governance of AI in Consequential Employment Decisions
New York City	L.L. 144 (enacted) (2021) L.L. 144 Rule (enacted) (2023)	Governance of AI in Consequential Employment Decisions
California	**CCPA Draft Regulations**	Comprehensive Data Privacy
Minnesota	**Minnesota Consumer Data Privacy Act**	Comprehensive Data Privacy
Utah	SB 149 (enacted) (2024)	Technology-specific (Generative AI)
California	AB 2013 (passed, awaiting signature) (Aug. 27, 2024)	Technology-specific (Generative AI)
California	SB 942 (passed, awaiting signature) (Aug. 19, 2024)	Technology-specific (Generative AI)

Executive Summary

1. **State lawmakers are primarily focused on regulating AI used in consequential decisions** that significantly impact individuals' livelihood and life opportunities.

- "**High-risk artificial intelligence system**" was used in at least seven proposals in 2024.
- "**Automated decision[making] tool**" or "technology" was used in at least ten proposals in 2024.
- "**Rights-Impacting Artificial Intelligence**," (The Office of Management and Budget)
- "**High-Impact AI Systems**" (bipartisan federal "Artificial Intelligence Research, Innovation, and Accountability Act of 2023")

Sector-Specific Laws and Proposals

Instead of broadly addressing "consequential decisions," some proposals and laws concentrate on specific sectors where automated systems are used.

- AI in employment: New York City Local Law 144 (enacted) and Illinois HB 3773 (enacted) (2024)
- AI in healthcare, as exemplified by Georgia HB 887 (proposed) (2024).

Executive Summary

Regulating AI used in consequential decisions:

- The **most debated and difficult factor** for U.S. state lawmakers to decide on has been the impact and role the AI system must play in the decision-making process in order for it to be in scope of regulation.
  - **Industry representatives** argue that broader thresholds could unintentionally regulate low-risk and essential technologies like calculators or Excel spreadsheets, which are not typically considered AI.
  - **Civil society and civil rights groups** argue that narrow thresholds may enable organizations to evade regulatory responsibility by merely having humans rubber-stamp decisions, failing to meaningfully address the many ways in which AI systems can result in discriminatory outcomes

Lawmakers often focus on three key terms:

Controlling Factor	Substantial Factor	Facilitating
Highest Threshold	Median Threshold	Lowest Threshold

Executive Summary

2. **A key goal for many lawmakers is to mitigate the risk of algorithmic discrimination,** either through:

Prohibition	Duty of Care
California AB 2930	**Colorado AI Act**
Deployers are prohibited from using an automated decision tool and prohibit developers from making available an automated decision tool if an impact assessment "identifies a reasonable risk of algorithmic discrimination (July 2024) - OR - Deployers are prohibited from using automated decision tools that resulted in algorithmic discrimination (February 2024)	Developers and deployers are subject to a duty to 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.

Executive Summary

Most AI legislative frameworks create role-specific obligations, including separate requirements for developers and deployers related to transparency, risk assessments, and AI governance programs.

Other measures: Audits

Tests an AI system to evaluate technical aspects based on particular metrics such as accuracy and reliability, usually for bias based on protected characteristics. (*E.g.* New York City Local Law 144)

Common concerns:

- Lack of standardization (NIST process ongoing)
- Diverging standards from civil rights
- Oversight of auditing industry

Alternative Approaches: Regulating Government Entities

Most states that address private sector regulation typically start by focusing on the use of AI or automated systems by government agencies. For AI in "consequential decisions," government use of AI often includes critical areas such as access to government benefits and criminal justice. This approach is exemplified by Maryland SB 818 (2024), Connecticut SB 1103 (2023)

Executive Summary

Common consumer rights around AI include rights of notice and explanation, correction, and to appeal or opt-out of automated decisions.

Alternative Approaches: Application and Updates to Data Privacy Laws:

Instead of introducing stand-alone AI proposals, some lawmakers have included similar protections in newer state privacy laws.

- **Minnesota Consumer Data Privacy Act (MNCDPA)** grants individuals the right to "question the result" of significant profiling decisions, challenge profiling results, understand the reasons behind decisions, and learn about possible actions to achieve different outcomes.

- **California Privacy Protection Agency (CPPA)** is in a pre-rulemaking process that would extend the application of the California Consumer Privacy Act to “automated decisionmaking technologies.”

Executive Summary

Alternatively, some lawmakers utilize a technology-specific approach to address novel risks.

The two most common specific technologies lawmakers have targeted are:

1. **Generative AI Systems** (AI that can create new content such as text, images, music, or videos) and
2. **Frontier AI or Foundation Models** (large AI models that can be used in a wide variety of use cases and applications, sometimes referred to as “general-purpose AI”)

The Technology-Specific Approach: Generative AI

Focus: Enhancing Transparency about Generative AI inputs, use, and outputs

- **Utah SB 149 (Enacted):** Requiring individuals or entities to clearly and conspicuously disclose when a generative AI system is interacting with a consumer in certain consumer contexts protected by UDAP

- **California**
  - 2018 law that prohibits using a "bot" to communicate or interact with the intent to mislead individuals about the bot's artificial identity
  - **AB 2013** (Passed, Awaiting Governor Action) would mandate that developers of generative AI systems publicly disclose documentation about the **data** used to train these systems.
  - **SB 942** (Passed, Awaiting Governor Action) would require entities providing generative AI tools to offer an "**AI detection tool**" that lets individuals check whether content was created or modified by the AI system

The Technology-Specific Approach: Frontier or Foundation Models

Focus: Incentivizing safety and mitigating catastrophic risks

- California SB 1047 (Passed, Awaiting Governor Action) would require developers to certify to the government that their frontier models have a written “safety and security protocol” and the capability to promptly enact a “full shutdown” if needed.

Considerations on Frontier/Foundation Models:
Challenges stem from the complexity and scale of these models, their diverse range of applications, and the technical expertise required to develop effective regulatory standards. Additionally, derivative AI systems can be built based on foundation models through a process of “fine-tuning” the model to perform specific functions. Two major questions have arisen for policymakers:

- **Computational thresholds** - what should they be? are these good indicators of risk?
- **Supporting open source**

Questions?