

Trends in U.S. State AI Legislation

*A Look at How U.S. State Policymakers Are Approaching
Artificial Intelligence Regulation*

[Preview of Future of Privacy Forum Legislation Report](#)

Future of Privacy Forum

The Supporters

220+

Member
Companies

55+

Leading
Academics

20+

Advocates and
Civil Society

5

Foundations

The Mission

The Future of Privacy Forum (FPF) is a global non-profit organization based in Washington, DC that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of emerging technologies and data uses, identify the risks, and develop appropriate protections.

We are optimists who believe technology and data can benefit society and improve lives if the right laws, policies, and rules are in place.

Trends in U.S. State AI Legislation

FPF Forthcoming Report “A Look at How U.S. State Policymakers Are Approaching Artificial Intelligence Regulation”

Key Takeaways

~33
States That
Introduced
Relevant AI Bills

~112
Relevant State
AI Bills

17
Enacted AI Bills

11
Key State AI Bills

1. **The Risk-Based Approach** To Regulating AI Systems Is Most Prevalent Across State Legislative Proposals, Focusing on AI Systems Used in Consequential Decisions that Impact Individuals.
2. Most Frameworks Have Provisions Regarding **Algorithmic Discrimination**
3. **There are Typically Role-Specific Responsibilities** That Reflect The Distinct Roles And Capabilities Held By Developers And Deployers.
4. **Common Consumer Rights** Include Rights Of Notice And Explanation, Correction, And To Appeal Or Opt-Out Of Automated Decisions.

Why State Lawmakers Looked to Regulate

- **Protecting Privacy and Data Security:** AI relies on vast amounts of personal data, creating a heightened risk of privacy breaches. Lawmakers aim to ensure that AI systems handle personal information securely and transparently, protecting citizens' privacy rights.
- **Ensuring Fairness and Preventing Discrimination:** AI systems can unintentionally perpetuate biases present in their training data, leading to discriminatory outcomes. Regulations aim to ensure that AI systems are fair, equitable, and do not discriminate against individuals based on race, gender, or other protected characteristics.
- **Enhancing Transparency and Accountability:** AI decision-making processes can often be opaque, making it difficult for individuals to understand how decisions that affect them are made. Regulations seek to enhance transparency, ensuring that AI systems are accountable and that their decision-making processes can be scrutinized and understood.
- **Promoting Ethical AI Development and Use:** State lawmakers aim to establish ethical guidelines for the development and use of AI to ensure that these technologies are aligned with societal values and public interest.
- **Supporting Innovation and Competitiveness:** By providing clear regulatory frameworks, states can foster a stable environment for AI innovation. This can attract investment and talent, helping states remain competitive in the rapidly evolving tech landscape.
- **Addressing Safety and Security Concerns:** AI systems, particularly those used in critical infrastructure, healthcare, transportation, and law enforcement, must be reliable and secure. Regulations aim to ensure that these systems are safe and do not pose undue risks to public safety.

Overview of Approaches

- 1. Risk-Based Approach:** This approach focuses on identifying and regulating “high-risk” AI, i.e. automated tools used in the context of high-risk decisions
- 2. Technology or Sector-Specific Approach:** This approach involves regulation of particular AI technologies, such as generative AI, or regulating AI applications within specific contexts, such as employment or within government agencies
- 3. Updates to Existing Laws:** this approach aims to amend existing laws such as state privacy, anti-discrimination, or unfair and deceptive trade practices to explicitly account for AI and automated decisionmaking systems

Takeaway 1: The Risk-Based Approach To Regulating AI Systems Is Most Prevalent Across State Legislative Proposals

Developers and **Deployers** of AI systems or tools used in **high-risk decision-making contexts** that significantly impact individuals' livelihood and life opportunities.

(1) The Context of Decisions In Which The Law Should Apply—Typically Areas Protected By Civil Rights Laws And/Or Essential To Individual Livelihoods

The decision must have a **legal or similarly significant effect** on the **provision or denial of**:

- Education enrollment or an education opportunity;
- Employment or an employment opportunity;
- Housing;
- A financial or lending service;
- An essential government service;
- Healthcare services;
- Insurance; and
- Legal

Plus, some common exceptions, including:

- Technology exceptions
- Existing Law Exemptions
- Small Business Exemptions
- Public Interest Exemptions

(2) The Impact And Role Of AI System On The Decision

Controlling Factor	Substantial Factor	Facilitating
Highest Threshold	Median Threshold	Lowest Threshold

Takeaway 2: Most Frameworks Have Provisions Regarding Algorithmic Discrimination

“Algorithmic Discrimination” is a condition where the use of an AI system results in unlawful or unjustified differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived protected class.

Duty of Care	Prohibition
Colorado AI Act	California AB 2930
<p>Prohibit deployers from using an automated decision tool that results in algorithmic discrimination;</p> <p>Prohibits developers from making available an automated decision tool if an impact assessment “identifies a reasonable risk of algorithmic discrimination”</p>	<p>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.</p>

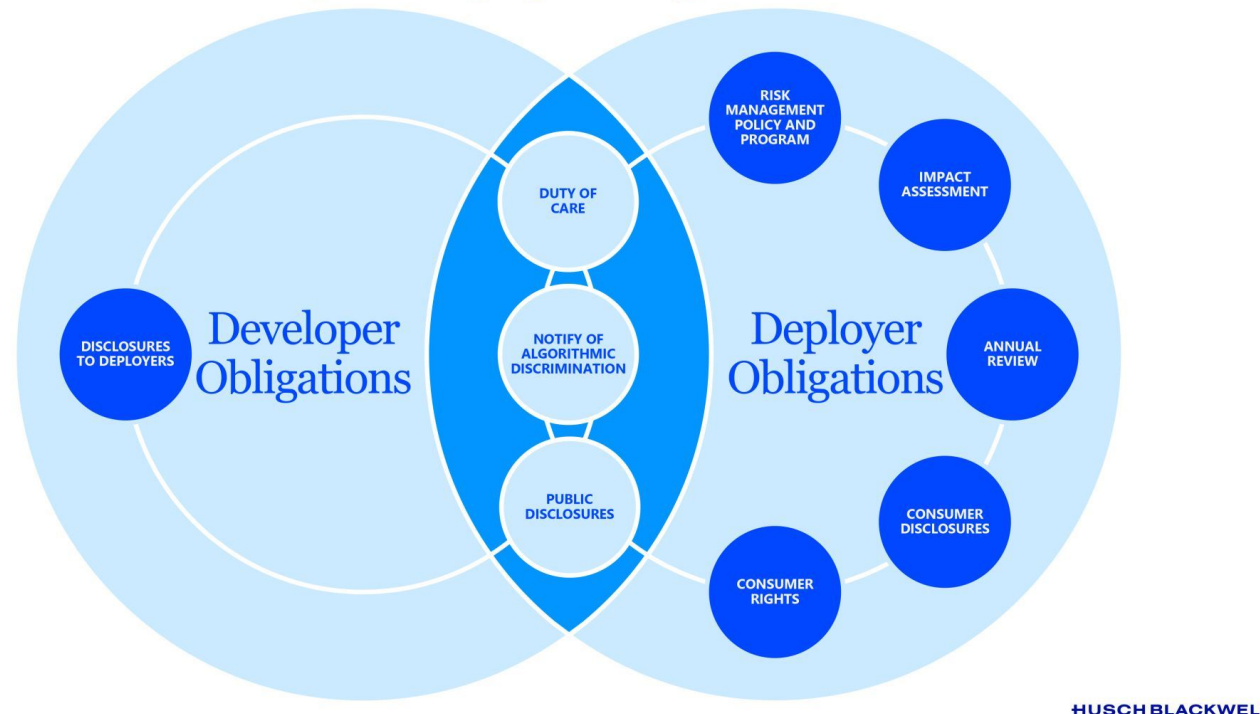
Takeaway 3: There are Typically Role-Specific Responsibilities That Reflect The Distinct Roles And Capabilities Held By Developers And Deployers

Developer:

Generally, the persons or entities that are developing, or creating, an AI system.

- Determine the purpose and scope of the AI system;
- Gather and preprocess data to train the model;
- Choose or design the appropriate algorithm or model architecture;
- Train the model;
- Conduct necessary evaluation and optimization.

Colorado AI Act: Developer v. Deployer Obligations



Deployer:

Generally, the persons or entities that are deploying or using an AI system.

- Integrate the AI system into the existing infrastructure;
- Monitor the system for any issues or necessary updates;
- Manage the deployment pipeline, including version control and rollbacks.
- Interface with consumers or users subject to AI decisions

Takeaway 3: There are Typically Role-Specific Responsibilities That Reflect The Distinct Roles And Capabilities Held By Developers And Deployers

Common Developer and Deployers Obligations

Transparency

Notice to Public: Requires developers and deployers to provide publicly available information about AI systems developed and used.

Notice To Individuals: Requires deployers to provide certain information to people subject to automated decision-making technology or consumers interacting with AI products, such as what the system is used for and how it works.

Assessments and Documentation

Risk/Impact Assessment: Requires a developer and/or a deployer to conduct an assessment regarding a system's purpose, limitations, and safeguards, and document whether and to what extent an AI system poses a risk of harm to individuals.

Documentation Between Parties: Requires developers to share information with deployers about an AI tool, such as the purpose and limitations, how it was created, testing conducted, and risk mitigation measures. Developers may be required to also assist deployers in their obligations. Deployers may also be required to report instances of algorithmic discrimination identified.

AI Governance Programs

AI Governance Programs: Requires developers and/or deployers to create a structured or semi-structured framework of policies, procedures, and controls designed to oversee and manage the development, deployment, and use of AI within an organization.

Takeaway 4: Common Consumer Rights Include Rights Of Notice And Explanation, Correction, And To Appeal Or Opt-Out Of Automated Decisions.

Right to Notice and Explanation

Most risk-based approaches acknowledge the need for individuals to **know that an automated system** is being used before it is used on them, how and why it is being used, and/or information to be disclosed to the individual that explains the when an adverse decision was rendered by the automated decision system.

Adverse Decision Notice

If an adverse decision is made by an AI system, some proposals and sector-specific laws require additional information to be disclosed to the individual that explains the when an adverse decision was rendered by the automated decision system.

Right of Correction

Because automated decisionmaking systems can make errors or rely on incorrect or outdated data, some proposals require deployers to provide individuals an opportunity to correct any incorrect personal data processed in an automated decision system, if an adverse decision was rendered.

Right to Opt-Out

Proposals with opt-out rights allow individuals to request not to be subject to a covered decision made by an automated system before the system is deployed against them.

Right to Appeal

Proposals with a right to appeal allow individuals, after an adverse decision is reached, to request that the adverse result rendered by an automated system be reviewed by a human.

Additional Content in the Report

How Some Lawmakers Are Updating Or Introducing Novel Provisions In Data Privacy Laws To Account For AI

Bills Regulating Government Agency Use of AI

Provisions Promoting Interoperability with the EU AI Act and NIST AI Risk Management Framework

Enforcement and Investigation Issues

Intersection with Existing Civil Rights Laws

Approaches to AI in Employment

Balancing Consumer Transparency and Business Trade Secrets

Approaches To Regulating General-Purpose, Foundation, And Generative AI Models.

First Amendment Considerations

Questions?



Tatiana Rice,
Deputy Director,
U.S. Legislation at
Future of Privacy Forum

trice@fpf.org