

Holistic AI Insight Paper

Regulation of AI and Algorithms in the US:

# Federal, State-level and Local Approaches

---

November 2022



**Holistic AI**

HOLISTICA.I.COM

# CONTENTS

---

## **3** INTRODUCTION

### **3** THE ROLE OF GOVERNANCE

## **4** FEDERAL-LEVEL INITIATIVES

### **4** THE ALGORITHMIC ACCOUNTABILITY ACT

### **5** THE AI BILL OF RIGHTS

### **6** NIST'S RISK MANAGEMENT FRAMEWORK

### **7** FTC REGULATION & READING BETWEEN THE LINES

## **8** STATE-LEVEL INITIATIVES

### **9** PASSED LEGISLATION

#### **9** Illinois Artificial Video Interview Act

#### **9** New York City Mandatory Bias Audits

#### **9** Colorado Restrict Insurers' Use of External Consumer Data Bill

### **11** PENDING LEGISLATION

#### **11** California Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems

#### **11** California Workplace Technology Accountability Act

#### **11** DC's Stop Discrimination by Algorithms Act

#### **12** Beyond the Technology Belt

## **15** NEXT STEPS

---



## KEY TAKEAWAYS

- In the United States, AI is being adopted across all sectors and can offer many benefits.
- However, AI can pose novel risks that must be acknowledged and managed.
- AI governance is one way to manage these risks and legislation that codifies this is starting to emerge in the US.
- AI regulation in the US is emerging across all sectors but particular focus has already been placed on HR tech and insurance.
- The US approach is not a one-size fits all top-down approach; instead, central verticals such as privacy and bias are paving the way for individual states and localities to tackle AI risk.
- AI regulation in the US is not just confined to legal authorities; guidance, frameworks and rulings have been published by multiple authorities including the Federal Trade Commission and the National Institute of Standards and Technology.
- AI legislation is not just seen in “techy-savvy” states such as New York and California, but across the US, states like Kentucky, Massachusetts, and Michigan, New Jersey, are pushing the agenda forward as well.
- It is important to get ahead of this regulation and get compliant.



# INTRODUCTION

Artificial intelligence (AI) refers to systems or algorithms that use human-defined objectives to generate outputs that can influence real and virtual environments, including content, predictions, recommendations, or decisions. It is applied across sectors and can offer many benefits, such as increased efficiency and accuracy. However, AI poses novel technical, legal and ethical risks and can harm system users if these risks are not managed.

Across sectors, we have already seen some high-profile [examples](#) of the harm that can result from AI and algorithms if their risks are not properly managed:

- [Amazon's resume screening tool](#) was retired before being deployed since it was biased against female candidates who included the word "women's" (e.g., "women's college") in their resume.
- Northpointe's tool COMPAS, which was designed to predict the likelihood of a criminal reoffending, was also found to be [biased](#) against black defendants, predicting them to be at a higher risk of recidivism than they were.
- The algorithms used to determine car insurance premiums in the US gave residents of predominantly minority areas [higher quotes](#) than those living in non-minority areas with similar levels of risk.

## THE ROLE OF GOVERNANCE

One of the key ways to manage the risks of AI is by ensuring that AI has the appropriate [governance](#) to manage both the technical and non-technical risks. Technical governance concerns systems processes that make the technology more accountable and transparent - including justifying design choice, while non-technical governance concerns systems and processes that focus on training and education and ensuring appropriate human oversight.

Legislation can help to ensure that AI systems and algorithms are developed and deployed lawfully. However, while existing laws somewhat apply to AI, such as privacy laws regulating data use, they alone are insufficient to prevent AI from causing harm. Consequently, countries worldwide are starting to crack down on AI to manage and prevent harm. One of the countries playing an active role in regulating AI design, development, and deployment is the United States (US), where efforts are being seen at Federal, state, and local levels.

# FEDERAL-LEVEL INITIATIVES

Several initiatives to regulate AI and algorithms have been proposed at the federal level. While not all of these initiatives are binding, they demonstrate that AI regulation is a priority for multiple authorities in the US. The main initiatives are:

- The Algorithmic Accountability Act – a Bill introduced to congress that would require impact assessments of automated systems and transparency about how they are used.
- Blueprint for an AI Bill of Rights – a non-binding framework published by the Whitehouse to guide the design, use, and deployment of automated systems.
- NIST's Risk Management Framework - The National Institute of Standards and Technology's soft law based on the governance, mapping, measuring and management of risks.
- Application of the FTC's regulation – some regulations imposed by the Federal Trade Commission extend to the use of AI.

## THE ALGORITHMIC ACCOUNTABILITY ACT

First introduced in 2019, the Algorithmic Accountability Act of 2022 (AAA) was reintroduced into both houses of Congress in February 2022. If passed, the Act would be binding and require companies to assess the impact of the automated systems they use and sell in terms of bias and effectiveness. Documentation from impact assessments would be required to be submitted to the Federal Trade Commission (FTC). Companies would also be required to be more transparent about when and how automated systems are used. This would apply to any person, partnership, or corporation that uses an automated system to make critical decisions if they have more than \$50 million in annual revenue and possess, manage, modify, handle, analyse, or control the data of more than 1 million people.

The FTC would enforce this legislation by developing assessment and reporting guidelines and providing annual anonymised aggregated reports on trends using the submitted documentation. The FTC would also have the power to conduct audits of AI systems developed by vendors and AI systems

used by companies for decision-making. The FTC would establish a Bureau of Technology that employs 50 staff to support this.

The Act has yet to win support in the House or the Senate and is not expected to pass, with the [EU AI Act](#) set to become the global gold standard for AI regulation. However, its introduction signals the intent of U.S. lawmakers, which is reinforced by the other federal initiatives on AI governance.

## THE AI BILL OF RIGHTS

The Whitehouse recently published a Blueprint for an [AI Bill of Rights](#) to guide the design, deployment, and development of AI systems. The Blueprint is non-binding and relies on designers, developers and deployers to voluntarily apply the framework to protect US Americans from the harms that can result from the use of AI.

The agenda adopts [five principles](#) to address these concerns:

- **Safe and effective systems** – steps to ensure that users are protected against unsafe and ineffective systems, including adherence to standards and ongoing monitoring.
- **Algorithmic discrimination protection** – proactive and continuous action should be taken to prevent algorithms from unfairly discriminating against particular groups through protecting against the use of proxy variables and ensuring that datasets are representative.
- **Data privacy** – there should be built-in protections against abusive data practices, and users should have agency about how their data is used.
- **Notice and explanation** – informing users that an automated system is being used and how and why it will have an impact on relevant outcomes.
- **Human alternatives, consideration and fallback** – users should be able to opt-out of the use of automated systems and should be able to receive support to resolve any issues that are encountered with the system.

The Blueprint is also accompanied by a [technical companion](#), a handbook to support the implementation of the principles outlined by the framework. The document, From Principles to Practice, is based on insights from researchers, technologists, advocates, and policymakers and gives examples of how the guidance can be applied to different AI technologies.





# NIST'S RISK MANAGEMENT FRAMEWORK

The National Institute of Standards and Technology (NIST) is a US government agency known for its soft law approach governing emerging and critical technologies. [The AI Risk Management Framework \(AI RMF\)](#) is the agency's soft law approach to AI in the US. The framework emphasizes the importance of context in AI regulation advisory instead of prescribing risk thresholds or values. The [framework](#) is made up of four core principles.

- **Govern** - Organizations must cultivate a risk management culture, including having the appropriate structures, policies, and processes. Risk management must be a priority for senior leadership.
- **Map** - Organizations must understand what their AI system is trying to achieve and the benefits of this compared to the status quo. By having a solid understanding of an AI system's business value, purpose, specific task, usage, and capabilities, organizations have helpful contextual information to decide whether to develop this system.
- **Measure** - If organizations decide to continue to develop their AI systems, then quantitative and qualitative methods should be employed to analyze and assess the risk of the AI system, along with how untrustworthy it is. Metrics and methodologies must be developed, as well as the involvement of independent experts. These metrics can help assess an AI system on the following lines: fairness, privacy-enhancing, transparency, explainable, safe, and reliability.
- **Manage** - Identified risks must be managed, prioritising higher-risk AI systems. Risk monitoring should be an iterative process, as post-deployment monitoring is crucial, given that new and unforeseen risks can emerge.

# FTC REGULATION & READING BETWEEN THE LINES

If the Algorithmic Accountability Act does pass, the FTC will complement it along with its own rules regarding the use of AI. This is significant as it demonstrates that it is not just the government acting to regulate AI, but other rule-making authorities are speaking up too with either new or applicable existing legislation.

As well as the FTC's proposed [Commercial Surveillance and Data Security](#) Rulemaking, which includes 95 data-related questions, 19 of which deal with automated decision-making and algorithmic discrimination, the FTC also has three Acts that have implications for companies that utilize AI in any form of their business practices:

- [The Federal Trade Commission Act 1914:](#) Section 5 of this legislation prohibits unfair or deceptive practices. According to the FTC, an example of this would be the sale or use of racially biased algorithms.
- [The Fair Credit Reporting Act \(FCRA\) 1970:](#) Created to protect consumer information and privacy as consumer reporting agencies collect this information. This law can be applied when an algorithm is used to deny people employment, housing, credit, insurance or other benefits.
- [The Equal Credit Opportunity Act \(ECOA\) 1974:](#) Created to make it illegal for a creditor to discriminate against a credit transaction based on the applicant's race, colour, religion, national origin, sex, marital status, or age. Under this law, it would be illegal for a company to use a biased algorithm that results in credit discrimination based on protected characteristics.

Compliance with the FTC's rules is critical, and it has already brought complaints against Facebook (now Meta) to hold it accountable for violating the 2012 Order and the FTC Act. [In this case](#), Facebook seemingly allowed consumers to opt into the company's facial recognition algorithm. Still, the algorithm was being deployed regardless of whether a consumer was opting in. [In another case](#), a California based-photo app, Everalbum, received allegations of deceiving consumers about the use of facial recognition and its data detention policy, with accusations that it retained the photos and videos of users who deactivated their accounts. A consent order was brought forth, and if made final, each following violation would carry a civil penalty of up to \$43,280 for Everalbum.



# STATE-LEVEL INITIATIVE

In the US, while there is currently no enforceable AI regulation at the Federal level, businesses employing AI must still be vigilant in complying with state-level regulation. Not just seemingly tech-savvy states like California or New York enforce compliance across different verticals but states like Colorado, Illinois, and Washington. Having more success than the federal initiatives, some local initiatives have already been enacted, and some are already in effect. Unlike the federal initiatives, which focus on broad applications of AI and aim to address multiple risks of AI, state and local legislation typically have a narrower focus. Currently, state-level enacted AI legislation is primarily concerned with managing bias and transparency risks and is targeted at specific sectors such as HR tech and insurance:

## HR TECH

- **Illinois Artificial Intelligence Video Interview Act** – requires employers to use AI to judge video interviews to inform candidates of this and the characteristics that will be considered.
- **NYC Bias Audit Mandate** – Employers using automated employment decision tools to make hiring or promotion decisions about employees or candidates in New York City must commission annual independent bias audits.
- **California Proposed Amendments to Employment Regulation Regarding Automated Employment Tools** – Extends employment regulations to prevent automated decision tools that discriminate based on protected characteristics from being used.
- **California Workplace Technology Accountability Act** – restricts electronic workplace monitoring, gives workers the right to access and request corrections of their data, and requires algorithmic and data protection impact assessments.

## INSURANCE

- **Colorado Restrict Insurers' Use of External Consumer Data Bill** – prohibits insurance providers from using data or algorithms that unfairly discriminate based on protected characteristics.

# PASSED LEGISLATION

## ILLINOIS ARTIFICIAL VIDEO INTERVIEW ACT

Legislation [already in effect](#) in Illinois requires employers to use AI to judge video interviews to inform candidates that AI will be used to judge their interview, how the AI works, and the characteristics it will use to make its decisions. Employers must also obtain consent from candidates to use the AI before the interview and are prohibited from sharing videos unless the technology or expertise of a third party is needed for analysis. Employers are also required to destroy videos within 30 days of receipt of a request from a candidate and must instruct any third parties who also have a copy to destroy any related material.

## NEW YORK CITY MANDATORY BIAS AUDITS

The New York City (NYC) Council has [mandated bias audits](#) and automated employment decision tools used to make hiring or promotional decisions about employees or candidates residing in the City. The first of its kind, the legislation also requires that candidates or employees are notified that such tool is being used and the characteristics being considered, therefore managing bias and transparency risks. [Recently proposed updates to the rules](#) also clarify how impact ratios, used to determine whether a system is biased, should be calculated and encourage intersectional comparisons.

## COLORADO RESTRICT INSURERS' USE OF EXTERNAL CONSUMER DATA BILL

In Colorado, AI is regulated in the insurance sector as a step to prevent discrimination. [The bill](#), Restrict Insurers' Use of External Consumer Data: Concerning Protecting Consumers From Unfair Discrimination in Insurance Practices, [requires](#) that insurance providers establish a risk management framework to prevent unfair discrimination in algorithms, predictive models, external customer data, and information sources based on protected attributes (race, colour, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity, or gender expression). Like the NYC and Illinois laws, the bill also has transparency requirements; insurers must outline the type of external customer data and information sources used by their algorithms and predictive models.



Legislation	Jurisdiction	Summary	Verticals
A Local Law to amend the administrative code of the city of New York, in relation to automated employment decision tools Transparency Law	New York City	Bias audits of automated employment decision tools; candidates must be informed of the use of the tool 10 business days prior to its use and the data used to make decisions	Bias, transparency
Artificial Intelligence Video Interview Act	Illinois	Candidates must be informed of the use of AI video interviews and the characteristics used to make judgements	Transparency
Concerning protecting consumers from unfair discrimination in insurance practices	Colorado	Bias audits of algorithms and data, maintenance of a risk management framework, explanation of how data and algorithms are used	Bias, transparency



# PENDING LEGISLATION

## CALIFORNIA PROPOSED MODIFICATIONS TO EMPLOYMENT REGULATIONS REGARDING AUTOMATED-DECISION SYSTEMS

In California, [Proposed Modifications](#) to Employment Regulations Regarding Automated-Decision Systems seek to regulate the use of algorithms and their capacity to discriminate against protected groups, extending existing [non-discrimination](#) laws. Employers with five or more employees are subject to this [regulation](#), which includes employees outside of California. Still, the act protections do not cover them if the illegal activity did not occur in California. In addition, vendors, or agents, acting on behalf of an employer are also considered an employer under this regulation and are therefore also liable for compliance.

## CALIFORNIA WORKPLACE TECHNOLOGY ACCOUNTABILITY ACT

California has also proposed a [Workplace Technology Accountability Act](#), which seeks to [limit workplace monitoring](#) to only specific activities and locations and requires employers to notify workers of monitoring, providing more transparency about monitoring. It would also give [workers more rights](#) in accessing the data their employer holds about them and requesting updates to data that is believed to be inaccurate. The Act would also require algorithmic impact assessments of automated decision systems and data protection impact assessments of work information systems to [identify risks](#) such as bias, the potential for mental and physical harm, and errors.

## DC'S STOP DISCRIMINATION BY ALGORITHMS ACT

Echoing the sentiment of the more sector-agnostic approach to AI regulation seen at the Federal level, Washington has proposed the [Stop Discrimination by Algorithms Act of 2021 \(SDAA 2021\)](#). The Act would prohibit algorithmic decision-making from utilizing subsequent determinations in a discriminatory manner. In addition, it would require annual bias audits to identify discriminatory outcomes associated with algorithmic decision-making systems. Finally, the Act would also impose transparency requirements, requiring that algorithmic systems notify individuals of their personal information use.

The Act would apply to any individual, firm, corporation, partnership, cooperative, or association that possesses or controls personal information on more than 25,000 District residents; has greater than \$15 million annual revenue; is a data broker that derives at least 50% of its annual revenue from collecting, assembling, selling, distributing, providing access to, or maintaining personal information, or who is a service provider. A [September public hearing](#) on the Act was held to clarify the legislation's requirements and objectives.

## BEYOND THE TECHNOLOGY BELT

States outside of the US's technology belt are following suit in aiming to pass AI regulation that mainly focuses on the verticals of discrimination and privacy. For example, [pending amendments](#) to existing legislation in Rhode Island will prohibit using algorithms and predictive models that use external data that unfairly discriminate, specifically in the context of insurance business practices. While like the aforementioned Colorado Insurance Law, the likelihood of these pending amendments passing is low given that the bill has been tabled by being motioned to hold for further study.

In Kentucky, [introduced legislation](#) will similarly prohibit violating an individual's constitutional rights based on predictive behaviour analysis, among others. A public hearing was recently held for this bill, and, like the SDAA 2021, it is underpinned by a determination to protect individual constitutional rights from automated discrimination.

However, not all proposed legislation is focused on prohibition; in Massachusetts, An [Act Establishing an Internet Bill of Rights](#) is currently pending. If passed, this would require relevant enterprises to disclose the use of automated decision-making, including if used for profiling endeavours. Enterprises would also have to provide meaningful information about the automation's logic and predicted consequences of the AI use, but what constitutes meaningful information is yet to be specified. In Michigan, [The proposed Employment Security Act](#) would require the review of algorithms and logic formulas used by the unemployment security agency. In New Jersey, [proposed legislation](#) seeks to prohibit certain discrimination by automated decision systems, particularly in the healthcare, insurance, and credit industries.

The table below provides a sample of a more holistic rendering of currently pending AI-specific legislation in the US.



Legislation	Jurisdiction	Summary	Status
Workplace Technology Accountability Act	California	Would require algorithmic and data protection impact assessments of both algorithmic and worker information systems to identify risks such as bias and privacy concerns	<u>Re-referred</u>
Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems	California	Would regulate the use of algorithms and their capacity to discriminate against protected groups	<u>Proposed</u>
Concerning protecting consumers from unfair discrimination in insurance practices	Washington DC	Would prohibit algorithmic decision-making from utilizing subsequent determinations in a discriminatory manner as well as require the notification to individuals of the use of their personal information	<u>Public Hearing Held</u>
People's Privacy Act	Washington DC	Would give individuals the right to know what personal information is being collected by companies and organizations; prohibiting the unauthorized sale or use of personal data. Would also prohibit the installation and use of facial recognition systems in spaces of public accommodation as well as the use of data to discriminate	<u>Re-introduced</u>







An act relating to credit & predictive analysis	Kentucky	Would prohibit the violation of an individual's constitutional rights based on predictive behaviour analysis in relation to credit	<u>Introduced</u>
An Act Establishing an Internet Bill of Rights	Massachusetts	Would require relevant enterprises to disclose the use of automated decision making, including if used for profiling endeavours	<u>Accompanied a Study Order</u>
The Employment Security Act	Michigan	Would require the review of algorithms and logic formulas used by the unemployment security agency	<u>Referred To Committee On Workforce, Trades, And Talent</u>
An Act concerning discrimination and automated decision systems	New Jersey	Seeks to prohibit certain discrimination by automated decision systems	<u>Re-introduced</u>





## NEXT STEPS

The US is taking decisive action to manage the risks of artificial intelligence at federal, state and local levels. Most of these efforts are underpinned by a focus on addressing bias and increasing the transparency of AI systems. The implications of this are clear: companies that employ AI must be ready to tell the world what they are doing, the risks their systems might pose, and the steps they are taking to minimise these risks.

Taking steps to address the risks of AI early is the best way to get ahead of these upcoming regulations. Holistic AI has pioneered the field of AI Risk Management and empowers enterprises to adopt and scale AI confidently. Our team has the technical expertise needed to identify and mitigate risks, and our policy experts use that knowledge of and act on proposed regulations to inform our product. [Get in touch](#) with a team member or [schedule a demo](#) to find out how we can help you comply with these legislative requirements.



**GOT QUESTIONS OR WANT TO  
SCHEDULE A CHAT? CONTACT US AT**



**holisticai.com**



**we@holisticai.com**



**Holistic AI**

© 2022 Holistic AI. All rights reserved.