

Insights

A SURVEY OF THE US AI REGULATORY LANDSCAPE

Sep 12, 2023

As companies increasingly integrate AI into their products, services, processes, and decision-making, they need to do so in ways that comply with the different laws that have been passed and proposed to regulate the use of AI across the US. To help businesses keep abreast of this rapidly changing compliance landscape, we have set out below a comprehensive look at the current state of regulation at the federal and state levels.

FEDERAL REGULATION OF AI

Although the US does not yet have a federal legal regime directed toward AI, there have been some notable legislative and agency efforts to regulate the use of AI.

Last year, for example, two proposed laws addressed AI regulation – the **American Data Privacy and Protection Act** (ADPPA) and the **Algorithmic Accountability Act of 2022** (AAA). Both bills require impact assessments for algorithms used to make decisions that pose an elevated risk of harm to individuals.

The ADPPA, which is an omnibus data privacy law, requires large data holders that use covered algorithms in a way that poses “a consequential risk of harm to an individual or group” to conduct an impact assessment.

Similarly, the AAA is a bill tailored to regulate AI and other automated decision systems and requires covered entities to perform impact assessments of augmented critical decision processes. Critical decisions are decisions that have a significant effect on an individual’s “life relating to access to or the cost, terms, or availability of,” for example, education, employment, essential utilities, reproductive services, healthcare or housing. Covered entities must also continuously test and evaluate privacy risks, risk-mitigation measures and current and historical system performance.

Although neither bill was reintroduced this legislative term, the ADPPA in particular still received **attention** from Congress this year.

Senate Majority Leader Chuck Schumer (D-NY) has developed the **SAFE Innovation Framework** to help guide responsible AI innovation, and, as he explained in a **recent speech**, he will convene a

series of “AI Insight Forums to lay down a new foundation for AI policy.” Schumer also signalled that addressing AI needs to happen quickly, indicating that these expert forums will accomplish “years of work in a matter of months”.

AGENCY EFFORTS

Despite the absence of a federal AI law, AI is not completely unregulated at the federal level.

A **joint statement** on AI was issued by the Consumer Financial Protection Bureau (CFPB), US Department of Justice (DOJ), US Equal Employment Opportunity Commission (EEOC) and Federal Trade Commission FTC in April 2023. The joint letter expressed the collective concern that AI has the potential to be used for discriminatory or anticompetitive purposes. The letter emphasised that existing legal regimes apply to the use of automated systems. In other words, just because a credit decision or a housing decision is made by a machine rather than a human, those laws apply just the same. The letter explains that agencies will vigorously use – and in some cases have already used – their authority to protect individuals’ rights regardless of whether legal violations occur through traditional means or advanced technologies, like AI.

The FTC, for example, has already used its enforcement authority several times, employing a powerful remedial tool known as algorithmic disgorgement (sometimes referred to as model deletion). This tool requires companies to delete ill-gotten data and the models or algorithms developed with that data. So, for instance, if the FTC finds that a company trained a large language model (LLM), such as GPT-3, on improperly obtained data, then the company will have to delete not only all the data but also all of the products developed from that ill-gotten data.

The EEOC provides further detail on its approach to AI and related technologies in its **technical assistance document**, which offers employers guidance on how to comply with the Americans with Disabilities Act when using AI tools.

Agencies like the **US Securities and Exchange Commission (SEC)** and **US Department of Health and Human Services (HHS)** are also taking AI regulation seriously, both proposing rules to address the use of AI technology.

So while no new federal legislation has passed yet, federal agencies have made clear that they are paying attention to AI and are motivated to enforce the laws available to them. Indeed, FTC Chair Lina Khan has **said** that the FTC “will vigorously enforce the laws [they] are charged with administering,” and that she did not want to make the same mistakes with this technology as were made during the beginning of the Web 2.0 era of the mid-2000s.

STATE DATA PRIVACY LAWS

There are currently 10 states that have passed omnibus consumer privacy laws broadly regulating the collection, use and disclosure of personal data. Most of these laws also have provisions addressing automated decision-making, including AI, for “critical decisions”, which typically include decisions concerning housing, credit, employment, criminal justice or other decisions with significant effects. Common requirements for AI-based decision-making use include providing proper notice to consumers (e.g., what personal data the business is collecting and why), the ability to opt-out of automated decision-making, and data protection impact assessments.

States have also passed a number of AI-specific laws. Illinois became the first state to enact restrictions with respect to the use of AI in hiring when it passed the **Artificial Intelligence Video Interview Act**, which became effective in January 2020. The act requires employers using AI-enabled assessments to, among other things, notify applicants of AI use, explain how the AI works, obtain applicant consent and, when requested, destroy all copies of the applicant’s videos. After using AI, employers must annually report a demographic breakdown of the applicants they offered an interview, those they did not, and the ones they hired.

Maryland passed a **law** – which became effective in October 2020 – that prohibits an employer from using facial recognition for the purpose of creating a facial template during an applicant’s pre-employment interview, unless the applicant agrees by signing a consent waiver.

Finally, in 2021, Colorado enacted a law to protect consumers from unfair discrimination in insurance rate-setting mechanisms. The law applies to insurers’ use of external consumer data and information sources (ECDIS), as well as algorithms and predictive models that use ECDIS in “insurance practices” that “unfairly discriminate” based on certain characteristics. At the time of this publication, the regulations to implement the bill were still in the proposal stage.

Municipalities have also started to regulate the use of AI technologies in different contexts. New York City, for example, passed **Local Law 144**, which prohibits employers and employment agencies from using AI and algorithm-based technologies (referred to as AEDTs, or automated employment decision tools) for recruiting, hiring or promotion without those tools first being audited for bias. Enforcement of this law began in July 2023.

In 2023, state legislatures across the country responded to the growing impact of AI by introducing a substantial number of AI-specific bills. To date, approximately 43 bills have been introduced across 21 states that would regulate a businesses’ development or deployment of AI solutions. Of these, four omnibus consumer privacy laws have passed, while 21 bills failed to advance in the current legislative session. The remaining 18 active bills are currently awaiting further action or review by state legislatures.

Connecticut was the first to cross the finish line to regulate governmental use of AI. **SB 1103** was signed into law on 7 June and although the final bill is less ambitious than what was originally

proposed, Connecticut has made a huge step towards the regulation of government AI procurement and has laid the groundwork for the Connecticut legislature to pass a private sector AI bill next year.

WHAT SHOULD LEGAL/COMPLIANCE PROFESSIONALS DO?

- **Education.** Work with internal stakeholders to develop an inventory of all AI systems developed and used by the organisation. Pay particular attention to AI systems that make or substantially assist with outcome determinative decisions in the areas of employment, credit, healthcare, insurance, housing, criminal justice and the delivery of essential goods and services.
- **Compliance.** Evaluate whether the organisation's development or use of AI systems triggers compliance obligations under state or federal laws.
- **Governance.** Develop frameworks, policies and best practices for the responsible development and use of AI systems that are right-sized to the potential risks posed by your organisation's particular use of AI.

This may sound daunting, and no doubt organisations will need to adapt their existing internal compliance processes in order to meet the challenges of this rapidly changing compliance landscape. But, the good news for organisations is that there are many parallels to data privacy compliance work. Organisations can – and should – design their AI governance program on top of their existing privacy compliance framework and leverage many of the same processes like data inventory, data protection impact assessments and notices.

This article was first published in [Global Data Review](#).

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM



Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com

+1 415 675 3448

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.