

Regulating AI: Litigation Questions And State Efforts To Watch

By **Jennifer Maisel** (August 2, 2023, 11:40 AM EDT)

This second part of a two-part series on U.S. regulation of artificial intelligence systems highlights state legislation and litigation to watch concerning AI systems, and provides practical takeaways as we look toward the future. The first part of the series **provided an overview** and modern context for the existing federal regulatory, legal and risk management landscape for AI systems in the U.S.



Jennifer Maisel

State Regulation of AI

State legislatures have enacted several laws targeting AI technology, with many more proposals under consideration.

Much of the state-level AI legislation thus far has concerned specific applications of AI technology or use of AI in high-risk industries.

As summarized below, we have seen regulations targeting AI technology in law enforcement, autonomous vehicles, employment and hiring, insurance, and in the creation of involuntary pornography, among other areas currently up for debate:

- Several jurisdictions enacted facial recognition software bans or otherwise restricted the sale of facial recognition technology to law enforcement agencies, particularly in response to nationwide protests for racial equality and the litigation surrounding Clearview AI's development and use of facial recognition software.
- Nevada was the first state to adopt legislation concerning the testing of autonomous vehicles in 2011, creating a regulatory sandbox for innovation.
- In the employment context, Illinois enacted the Artificial Intelligence Video Interview Act to regulate the use of AI-enabled assessments that may result in bias in hiring decisions, Maryland's H.B. 1202 prohibits employers from using a facial recognition service during a preemployment interview absent applicant consent, and New York City Local Law 144 requires employers to conduct bias audits of AI tools used for employment decisions.
- California's Bolstering Online Transparency law went into effect in July 2019, and imposes notice and disclosure requirements where chatbots are used to incentivize a sale or transaction of goods or services or influence a vote in an election.
- In 2021, Colorado enacted S.B. 21-169, Protecting Consumers from Unfair Discrimination in Insurance Practices, which applies to algorithms and predictive models that use external

consumer data and information sources in insurance practices that unfairly discriminate.

- Several jurisdictions have also enacted laws allowing residents to sue the creators of deepfakes in civil court, particularly when it comes to involuntary deepfake pornography.

In the absence of comprehensive federal privacy and data protection laws, states are increasingly enacting omnibus privacy and data protection regulations that apply to AI technology that uses personally identifiable information. Some of these regulations further impose restrictions similar to Europe's General Data Protection Regulation concerning the use of personal information in automated decision making, particularly in high-risk industries.

A myriad of other state laws and regulations may affect AI technology, and even more in the pipeline as AI technology becomes more readily accessible for additional use cases.

Early Litigation

Several lawsuits are currently pending before the U.S. District Court for the Northern District of California and the U.S. District Court for the District of Delaware arising out of entities' use of copyrighted content and personal information to train AI models.[1]

These lawsuits may address issues of first impression, particularly as whether a defendant's use of copyrighted material to train a generative AI system is a defensible fair use.

Indeed, the Northern District of California, in *J. Doe 1 v. GitHub Inc.*, has already ruled in May that the plaintiffs have sufficiently stated at least one claim to survive a motion to dismiss.[2]

It is important to note that several of these litigations are putative class actions brought on behalf of broadly defined groups of people, including any person whose personal information a defendant used to train an AI system or whose copyrighted work a defendant used to train an AI system, and a final judgment could have significant implications for class members.

Critically, as demonstrated by these early cases, existing intellectual property, privacy, contract, unfair competition, and tort laws, among others, are potentially as equally applicable to AI systems as they are to anything else.

While AI systems may introduce novel questions as to the application of such laws to new facts, there is plenty of precedent, particularly from the cyberspace and digital context more broadly, from which to build a claim. These early lawsuits will further illuminate whether omnibus AI-specific laws are needed, or if existing laws can address the bulk of potential harms arising from AI systems.

As U.S. Circuit Judge Frank H. Easterbrook aptly noted in 1996 in the cyberspace context:

Beliefs lawyers hold about computers, and predictions they make about new technologies, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers.[3]

Practical Takeaways as We Look Toward the Future

In view of the existing legal and regulatory framework at both the federal and state level, enterprises should set up appropriate governance, policies, checkpoints and other guardrails to identify and address the risks posed by AI systems and to ensure that AI systems are, at minimum, safe, effective and lawful.

Those designing, developing and deploying AI systems should identify a standard framework to follow, update that framework as necessary and ensure ongoing compliance with that framework.

There are several standards, including the National Institute of Standards and Technology AI Risk Management Framework, to choose from, and is crucial to put in place appropriate governance,

policies and teams to maintain, update and enforce compliance.

A phase-in approach may be beneficial to test the fit of a new AI project along with a governance plane with separation of duties. AI systems are also unique from other software systems because of their reliance on data.

Accordingly, in order to identify any potential risks, enterprises should consider conducting audits on the data used to train an AI system in order to identify, for example, whether the data implicates any third-party intellectual property right or if the data includes any sensitive or personally identifiable information.

Additional compliance measures may be further required based on applications of an AI system in high-risk industries.

For those using AI systems, guardrails are necessary to ensure that the AI system is effective and is not resulting in biased, unfair, or otherwise untrustworthy decisions, particularly in high-risk industries.

In many instances, an enterprise may want to build in a human "gut check" to evaluate output from an AI system, and a mechanism to address an automated decision with a human reviewer.

Companies should address any confidentiality or security considerations at the outset of using any new AI system, particularly where employees may be using the AI system to analyze confidential or proprietary information. Avoid the black box trap by gaining an understanding of the training data, model design, assumptions and testing, and do not sign up for more red flags than you can handle.


The legal and regulatory landscape surrounding AI technology will undoubtedly continue to evolve.

In the meantime, one of the best assurances for the future is to take reasonable steps necessary to ensure that the benefits of AI technology far outweigh its risks.

Jennifer Maisel is a partner at Rothwell Figg Ernst & Manbeck PC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] J.L. et al. v. Alphabet Inc., et al., No. 23-cv-03440 (N.D. Cal. July 11, 2023) (putative class action on behalf of all persons whose personal information was used by the defendants or whose copyrighted works were used as training data for defendants' products); Silverman et al. v. OpenAI, Inc. et al., No. 23-cv-03416 (N.D. Cal. July 7, 2023) (putative class action complaint on behalf of copyright owners); Kadrey et al. v. Meta Platforms, Inc., No. 23-cv-03417 (N.D. Cal. July 7, 2023) (putative class action complaint on behalf of copyright owners); Tremblay et al. v. OpenAI, Inc. et al., No. 23-cv-03223 (N.D. Cal., Jun. 28, 2023) (putative class action complaint on behalf of copyright owners); P.M. et al. v. OpenAI, Inc. et al., No. 23-cv-03199 (Jun. 28, 2023) (putative class action complaint on behalf of individuals whose personally identifiable information was used by defendants); Getty Images (US), Inc. v. Stability AI, Inc., No. 23-cv-00135 (D. De. Feb. 3, 2023) (allegations surrounding unauthorized use of Getty Images' library of photos to train stable diffusion image generator); Andersen et al. v. Stability AI Ltd. et al., No. 23-cv-00201 (Jan. 13, 2023) (putative class action complaint on behalf of copyright owners); J. Doe 1 et al. v. GitHub Inc. et al., No. 22-cv-06823 (N.D. Cal., Nov. 3, 2022) (putative class action complaint on behalf of persons and entities that stored a copyrighted work on the GitHub platform under one or more open source licenses).

[2] **J. Doe 1 et al. v. GitHub, Inc. et al.** , No. 22-cv-06823-JST (N.D. Cal., May 11, 2023) (Dkt. 95, Order Granting in Part and Denying in Part Motions to Dismiss).

[3] Frank H. Easterbrook, "Cyberspace and the Law of the Horse," Chicago Unbound (1996 University of Chicago Law School), available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2147&context=journal_articles.

