

Legislation May Be Lacking, But AI Is Not A Legal Free-For-All.

By [Reiko Feaver](#) and [Beth Fulkerson](#)

May 19, 2023

Once upon a time, the internet was at the edge of the known world, wide open for opportunity and exploitation.

Chicken Little ran herself ragged — laws would fail, chaos would reign.

Now, we face another technological frontier: artificial intelligence. Scarier because it's not only new, but it's intelligent, and apparently, it doesn't need us. Laws will fail, chaos will reign.

The sky did not fall with the internet. Even without an existing body of internet law, the technology was tamed. How? With the old standbys, retooled to provide imperfect but passable guardrails.

The same is happening with AI. While artificial intelligence may be moving faster than internet speeds, it's not so new and unknowable that there isn't already a structure that has and will continue to be used for governance.

Companies using and developing AI, or considering getting in the game, are dangerously deluding themselves if they operate from the premise that minimal AI-specific legislation means an AI legal free- for-all.

Very Real Focus

In the U.S., the European Union and Canada, and across governments, nongovernmental organizations and private entities, a three-word AI foundational consensus has emerged: secure, trustworthy and ethical.

As written in the White House's AI Bill of Rights, the focal points are:

- Rights, including civil rights, civil liberties and privacy;
- Opportunities, including equal opportunities; and
- Access, including access to critical resources or services.

The EU's AI Act intends to ensure that AI systems in the EU are lawful, safe and respectful of fundamental rights and values.

Canada's AI and Data Act emphasizes governance and transparency.

The National Institute of Standards and Technology's Artificial Intelligence Risk Management Framework says trustworthy AI must be valid and reliable, safe, secure

and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair.

These principles, along with the AI Bill of Rights, make it clear which existing U.S. laws apply. Recent activities of regulatory agencies have added additional certainty.

On April 25, Federal Trade Commission Chair Lina M. Khan and officials from the U.S. Department of Justice, the Consumer Financial Protection Bureau and the U.S. Equal Employment Opportunity Commission released a joint statement on their enforcement efforts against discrimination and bias in automated systems.

Although it may seem silly to state that companies cannot use technology to break the law, the statement is important because it emphasizes the intent of these agencies to proactively use existing laws to ensure responsible development and use of automated systems.

Think Section 5 of the FTC Act, the Fair Credit Reporting Act, the Equal Employment Opportunity Act, the Equal Credit Opportunity Act, Fair Housing Act, Medicare, and laws and regulations enforced by the U.S. Department of Education.

Past actions, new rulemaking efforts and public discourse also provide guidance as to how the agencies intend to treat certain AI peculiarities.

Regarding the autonomy and intelligence of AI, the AI Bill of Rights, the FTC, the CFPB, the EU's AI Act, Canada's AI and Data Act, and various existing and proposed state legislation, emphasize that the AI must be accountable and transparent — the magic black box, head- in-the-sand argument will not fly.

The newness of AI leads to further definition of accountability and transparency, to include requirements that developers and deployers of these systems be able to identify how the AI was trained, potential risks of algorithmic discrimination, limitations, and what prerelease evaluation and testing measures were taken.

Proposed laws in South Carolina, Texas and New York require that the consumer have a fallback to an actual live person, as does the guidance in the AI Bill of Rights.

The FTC, the EEOC, the CFPB, the U.S. Department of Health and Human Services, the DOE and the U.S. Department of Housing and Urban Development have all taken regulatory actions relating to the use of automated systems and algorithms.[1]

The FTC has ordered companies to delete unlawful algorithms, and in August 2022, proposed rulemaking for commercial surveillance and data security.

In the overview of its proposed rulemaking, the FTC stated that companies' growing reliance on automated systems is creating new forms and mechanisms for

discrimination based on protected categories such as race, religion and sex, and that such discriminatory outcomes emerge even when unprotected consumer traits, such as place of education, are inputted into the systems.

The Near Future

In its May 2022 circular, the CFPB emphasized that the existing laws' transparency requirements are not weakened by the use of AI technology.

It directly answered the question of whether creditors are excused from complying with the Equal Credit Opportunity Act's requirement to inform applicants of the specific reasons why an adverse action was taken, when the decision is based on complex algorithms that prevent them from accurately identifying those specific reasons.

The answer was a resounding "No."

A creditor cannot justify noncompliance with ECOA and Regulation B's requirements based on the mere fact that the technology it employs to evaluate applications is too complicated or opaque to understand. A creditor's lack of understanding of its own methods is therefore not a recognizable defense against liability for violating ECOA and Regulation B's requirements.

Those laws that do exist and specifically focus on automated systems have, in large part, been crafted using consumer privacy concepts, focusing on disclosures, opt outs and impact statements.

While the transparency, fallbacks to a live person and disclosures bandied about in relation to AI echo these privacy concepts, newer proposed laws take more direct aim at the technology underlying automated systems and complex algorithms.

In particular, the newer proposals track the secure, trustworthy and ethical principles of responsible AI and the already-provided regulatory guidance.

These newer laws[2] will likely require developers and users of AI to provide quite detailed information regarding what went into creating the systems, including training data and processes and, importantly, will require developers and users to evaluate limitations and risks prior to deployment.

Those familiar with privacy by design will recognize the proactive approach to responsible AI.

Call to Action

Large language models and generative AI have propelled this technology into the popular spotlight and accelerated its development and use.

But regulators are already focused on ways to govern this new technology and are employing existing tools to reinforce the articulated AI governance principles noted above.

The obvious direction is that AI does not exist in a vacuum and companies must evaluate AI as with any corporate initiative.

At a minimum, smart companies will commence an AI inventory — as required of government agencies by Executive Order No. 13960 on trustworthy use of AI in the federal government — and identify where those systems might draw regulatory attention, such as credit, housing, employment and infringement of civil rights.

Smarter companies will start to treat AI use as with any corporate initiative, asking the same questions and moving forward with understanding and intention.

How did the initiative come about, and how was it created? What is its intended use? How does it achieve that use? What risks exist along that path? How do we mitigate those risks? And if someone asks, can we explain ourselves?

Enforced AI-specific laws will be here soon, but in the meantime the regulatory guidance of existing law, proposed laws and published industry frameworks provide companies enough fodder to begin to create, implement and maintain up-to-date governance processes and plans.[3]

At a minimum, keep the end goal in mind: AI must be secure, trustworthy and ethical.

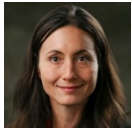
[1] See "The EU and US are starting to align on AI regulation": <https://www.brookings.edu/blog/techtank/2022/02/01/the-eu-and-u-s-are-starting-to-align-on-ai-regulation/>.

[2] As examples: CA: requiring deployers and developers of "automated decision tools" to file impact assessments setting out risks of algorithmic discrimination, training procedures, and pre-release evaluation for validity and explainability; notably, the law would mandate ongoing governance based on "map, measure, manage, and govern"; NYC's Use of AI in Hiring and Promotion (enforcement date extended to July, 2023) requires a publicly available, independent bias audit to include training methodology; NJ's proposed law also would require bias audits for use of AI in employment contexts; PA's proposed law would require information on the code used in the AI system; CO's Division of Insurance has already released a draft regulation requiring life insurers using algorithms or predictive models to establish a governance and risk management framework and setting out detailed required components of an acceptable plan; NJ's proposed law contains similar requirements. Note as well that certain legislation would more strongly regulate (including possibly prohibition absent compliance with strict

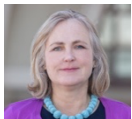
requirements) the use of AI in certain contexts, mirroring the risk-based approach that has been adopted in the EU AI Act and Canada's AI and Data Act. See IL, MA, MS, MD, SC, and TX.

[3] See NIST's Artificial Risk Management Framework; the Technical Guide for the White House AIBoR; and OECD's Recommendation of the Council on Artificial Intelligence.

The foregoing content is for informational purposes only and should not be relied upon as legal advice. Federal, state, and local laws can change rapidly and, therefore, this content may become obsolete or outdated. Please consult with an attorney of your choice to ensure you obtain the most current and accurate counsel about your particular situation.



[Reiko Feaver](#) is a partner and chair of the technology practice at Culhane Meadows Haughian & Walsh PLLC.



[Beth Fulkerson](#) is a partner and chair of the privacy, data and cybersecurity practice at the firm.

About Culhane Meadows – *Big Law for the New Economy*®

The largest woman-owned national full-service business law firm in the U.S., Culhane Meadows fields over 70 partners in eleven major markets across the country. Uniquely structured, the firm's Disruptive Law® business model gives attorneys greater work-life flexibility while delivering outstanding, partner-level legal services to major corporations and emerging companies across industry sectors more efficiently and cost-effectively than conventional law firms. Clients enjoy exceptional and highly-efficient legal services provided exclusively by partner-level attorneys with significant experience and training from large law firms or in-house legal departments of respected corporations. U.S. News & World Report has named Culhane Meadows among the country's "Best Law Firms" in its 2014 through 2023 rankings and many of the firm's partners are regularly recognized in Chambers, Super Lawyers, Best Lawyers and Martindale-Hubbell Peer Reviews.