



## No Loopholes for AI: Putting Legal Guardrails on Your Company's Use of AI

*Posted by Don L. Vieira and Nicola Kerr-Shaw, Skadden, Arps, Slate, Meagher & Flom LLP, on Wednesday, March 25, 2026*

**Editor's note:** Don L. Vieira is a Partner and Nicola Kerr-Shaw is a Counsel at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on their Skadden memorandum.

### Key Points

- While no comprehensive AI regulatory framework has been enacted in the U.S., the use of AI is governed by many existing laws, with new laws coming into force across the U.S. In their oversight roles, boards need to be aware of the spectrum of laws that may govern their companies.
- Existing laws and their application to companies need to be re-examined in light of AI advances, and new laws will need to be assessed against a business's AI needs and ambitions.
- With the rapid and prolific expansion of AI, companies need to implement agile and strategic compliance frameworks to keep pace with the business, and allow valuable and limited legal resources to be focused on those AI tools presenting the highest risk.

As board members, you've likely heard conflicting messages about artificial intelligence (AI) regulation in the U.S. Some claim that AI is simply not regulated in the U.S. The truth is more nuanced, and more immediately important, than you might think.

While it's true Congress hasn't passed sweeping AI-specific legislation, your company's use of AI is almost certainly regulated already. Here's why: The law doesn't care how you break the rules, only that you broke them.

### Deploying New Technology Doesn't Create Legal Immunity

Let's begin with a simple proposition: Using artificial intelligence to perform a task doesn't exempt you from the regulations that already govern that task. This principle seems obvious when stated plainly, yet sophisticated companies risk stumbling over it repeatedly.

Consider a financial services firm that deploys an AI system to evaluate loan applications. The Fair Lending laws — including the Equal Credit Opportunity Act and Fair Housing Act — will apply whether it is an algorithm making the decision or a loan officer. The fact that the discrimination may have emerged from biases built into a neural network rather than explicit human prejudices is likely irrelevant for purposes of the act.

This concept extends across every regulated sector. Health care companies using AI remain bound by the privacy and security obligations and standards of the Health Insurance Portability and Accountability Act (HIPAA), informed consent requirements and medical malpractice standards. Employers using AI screening tools for hiring must still comply with Title VII of the Civil Rights Act and the Americans with Disabilities Act. Public companies using AI to generate financial disclosures remain subject to securities law requirements for accuracy and completeness.

## Regulators Are Already Regulating AI – Sector by Sector

Industry regulators haven't been sitting idle while AI proliferates. They've been asserting jurisdiction over AI systems using their existing statutory authority — often in ways that create real enforcement risk and making it abundantly clear that their regulation and jurisdiction equally applies to AI.

The financial services sector illustrates this clearly. The Consumer Financial Protection Bureau has brought enforcement actions against companies whose algorithms produced discriminatory outcomes. The Securities and Exchange Commission has signaled heightened scrutiny of AI-driven trading systems. Banking regulators expect the same model risk management frameworks for AI that apply to traditional credit models, including robust validation, ongoing monitoring and clear governance.

In health care, the Food and Drug Administration now regulates certain AI and machine learning-based medical devices as software as a medical device (SaMD), requiring pre-market review for higher-risk applications. The Centers for Medicare and Medicaid Services has begun grappling with reimbursement policies for AI-enabled diagnostic tools. State medical boards are clarifying that physicians remain professionally responsible for AI-assisted clinical decisions.

Employment regulators are similarly engaged. The Equal Employment Opportunity Commission has issued guidance on AI hiring tools, emphasizing that employment discrimination laws fully apply regardless of whether a human or algorithm makes the selection. Several states and localities have gone further, enacting laws requiring specific transparency and audit requirements for automated employment decision tools.

## Why 'We Didn't Know What the AI Would Do' Isn't a Defense

Some companies assume that the “black box” nature of some AI systems creates plausible deniability for adverse outcomes. It doesn’t.

From a legal perspective, you are responsible for the systems you deploy. If a company puts an AI tool into production that affects customers, employees, patients, or investors, it owns the consequences. As regulators grapple with AI, it is becoming clear that saying “the algorithm did it” carries roughly the same legal weight as saying “the spreadsheet did it” or “the calculator did it.”

In fact, deploying systems you don’t fully understand may create additional liability. Regulators and courts expect companies to conduct appropriate due diligence before implementing technologies that affect people’s rights or economic interests and fully understand how they work and the potential risks they cause. If you cannot explain how your AI system makes decisions, you may struggle to demonstrate that you’ve met your duty of care or your obligation to ensure non-discriminatory outcomes.

This is particularly salient for board members. Directors have fiduciary duties to exercise reasonable oversight of corporate operations. Allowing the deployment of AI systems without adequate governance, testing, or monitoring could constitute a breach of the duty of care, especially if problems were foreseeable and preventable.

## The Compliance Framework

Rather than waiting for comprehensive federal AI legislation, boards should be asking management to implement governance frameworks now. Here’s what mature AI governance looks like in regulated industries:

**Define what you mean by AI.** The term AI encompasses a lot of technology, much of which is low risk and can be used with no additional concern or legal governance. So determine what type of AI, and what use cases, would actually trigger risks for your business (higher risk AI, such direct customer-facing AI tools with high reputational risk if they malfunction) and what systems your business absolutely relies on (key AI, such as a business-critical pricing system). This allows you to focus legal and compliance resources on the higher risk and key use cases.

**Inventory and risk classification.** You cannot govern what you don’t know exists. Companies need clear processes for identifying where higher risk and key AI is being used across the organization and classifying systems based on their risk profile. And, because AI tools’ risk often changes rapidly as new features are released and employees discover new uses for existing features, you also need processes to make sure that this inventory is kept up to date.

**Domain-specific compliance integration.** For each higher risk and key AI system, identify which existing regulations apply and build compliance requirements into the development and deployment process.

**Building on what you already have.** Integrate AI governance into existing compliance processes where possible, rather than “starting from scratch” with new AI policies that add complexity and don’t tie in to existing processes. For example, AI governance required to address anti-discrimination laws can be baked into existing anti-discrimination policies and processes, rather than siloed in an AI policy. Update your vendor management policy to deal with risks of vendors relying on AI when providing services to you, or using your data within the AI, rather than having a vendor section of an AI policy.

**Validation and testing protocols.** Before deployment, higher risk and key AI systems should be tested for accuracy, fairness and robustness. Many regulators also expect ongoing monitoring after deployment as well, since AI systems may drift over time.

**Human oversight and accountability.** While AI can augment decision-making, high-stakes decisions in regulated contexts typically require meaningful human involvement. Moreover, someone accountable must often be assigned responsibility for each AI system. You need to consider in what circumstances human oversight is required, what level of human oversight will occur, how you will train the humans delivering this oversight and (perhaps most difficult) how you will document that oversight. Regulators will expect to see evidence of what you’ve implemented and evidence that it is an appropriate level of human control.

**Transparency and explainability.** Even if you can’t fully explain every output of a complex model, you should be able to articulate what the system does, what data it uses, what it’s designed to accomplish and what guardrails exist, particularly methods to identify when AI has gone wrong and to rectify quickly. This matters for regulatory examinations, customer complaints and litigation.

## The Board’s Role: Ask the Right Questions

Board members don’t need to become AI experts, but you should be asking management pointed questions about AI governance:

- Do we have a comprehensive inventory of higher risk and key AI systems used across the organization, particularly in customer-facing or regulated functions?
- What governance framework ensures AI systems comply with applicable regulations before (and during) deployment?
- Who is accountable for higher risk and key AI systems, and do they have appropriate expertise in both the technology and the relevant regulatory requirements?

- What testing do we conduct, and what safeguards do we have in place, to ensure AI systems don't produce problematic outcomes? And if they do go wrong, how will we identify this quickly and rectify any errors?
- How do we monitor AI systems post-deployment?
- What training have employees received about appropriate AI use in their specific regulatory context?

## The Bottom Line

The absence of comprehensive federal AI legislation doesn't mean there is an absence of AI regulation. It means AI regulation is happening through the application of existing law — sometimes predictably, sometimes in novel ways that create uncertainty.

For boards, this reality requires active engagement. The risks aren't hypothetical. Companies have already faced enforcement actions, litigation and reputational damage from the deployment of AI systems. These risks will only intensify as AI adoption accelerates and regulators develop more sophisticated approaches to oversight.

The companies that will navigate this landscape successfully are those that recognize a simple truth: AI is a tool, and you remain responsible for what that tool does. Governance frameworks should reflect that reality, ensuring that innovation proceeds within the boundaries that law and regulation have established for your industry.