ALM | LAW.COM

New York Law Journal

TECHNOLOGY TODAY

ARTIFICIAL INTELLIGENCE

SHIELD: Guidelines for Navigating the AI Regulatory Landscape

By Katherine B. Forrest
August 18, 2025

Less than two years has passed since I started counseling companies on how to comply with a host of Artificial Intelligence (AI) regulations coming out of the European Union, the United States Federal Government and states.

But little is the same now as it was then. In this ever-changing AI regulatory landscape, it's hard to find some basic guidelines that can bring sense but also flexibility to compliance efforts. In this article I propose a set of guidelines that I call SHIELD.

S: Scope your AI systems and tools.

H: Highlight use cases and risk levels.

I: Identify applicable state, federal and international laws.

E: Establish oversight and accountability roles.

L: Log decisions, training data sources and disclosures.

D: Detect and respond to updates in the legal landscape.

SHIELD takes into account that U.S. companies have at least three sets of very relevant regulatory obligations–but all have shifted in the recent past, and more change is coming.

KATHERINE B. FORREST *is a partner at New York law firm Paul, Weiss, Rifkind, Wharton & Garrison LLP.*

Every state in the U.S. has introduced AI-related legislation and more than half have AI-related laws on the books.

Katherine B. Forrest

A number have laws relating to AI systems deployed for use cases that impact consumers–such as insurance claim processing, credit approval, employment application screening, and medical diagnostics.

Most such laws require some form of disclosure and testing for bias-related outcomes. Another set of laws relate to AI-generated video and audio content such as deepfakes, or political ads.

Adjacent to these laws are those that place restrictions on the ability of third parties to use someone's name, likeness and image. Some states have banned certain applications based on the domain (mental health) or age of the user.

Federal laws in the U.S. have gone through significant changes in the last year–with the Trump Administration's fulfillment of its commitment to repeal the Biden Administration's AI Executive Order.

The Biden-era order tasked federal agencies with coming up with regulations in the executive branch.

There has not been any wholesale replacement of these.

In terms of existing federal laws (apart from caselaw interpreting existing laws as it pertains to AI), there is the Take it Down Act, passed in May 2025, that prohibits the dissemination of non-consensual deepfake imagery.

Instead of regulating to prohibit, the federal government is taking a more affirmative adoption stance.

It has entered into several contracts with major developers for federal employees to use their chat products, and has suggested that federal lands and resources will be used to further adoption of U.S. AI technology.

Legislation is pending relating to enabling enhanced access to compute infrastructure to allow for wider model and tool development.

Notably, the Trump Administration's AI Action Plan that came out in July 2025, calls for a "try it first" approach to AI tools, and a review and possible repeal of state laws that may impede the competitiveness of AI companies in the international arena.

This is a far more "hands-off" approach to AI regulation than the U.S. had previously been heading towards.

Meanwhile, the E.U. AI Act has started to be implemented. As of Feb. 2025, use cases that fall within the unacceptable risk categories (such as social scoring, biometric surveillance in public places), are now actively banned. As of Aug. 2, 2025, the General Purpose AI Obligations (GPAI) have started to go into effect.

The GPAI requires that models comply with a number of transparency, governance and confidentiality requirements (the E.U. has the extensive GDPR privacy regime that remains in effect); existing models have a two year phase in period.

With more than 30-plus state laws, some federal regulation and potential roll-back of unspecified state laws, and E.U. laws that have extra-territorial reach, companies are left in a bit of a compliance quagmire. This is putting to the side that there are additional AI regulatory schemas in the Asia-Pacific region, the U.K., Brazil, etc.

Keeping up with all of the regulatory requirements, and changing obligations, is a challenge indeed. The SHIELD guidelines I suggest above are one way to think about it. (Of course, this article cannot and is not intended to give legal advice; SHIELD is just for possible consideration).

The "S" in SHIELD is for companies to *scope* their AI systems and tools–to have an inventory at-the-ready that provides a knowledgeable starting place for all compliance actions that may need to follow.

The "H" requires a company to obtain sufficient information about its use cases – to *highlight* those use cases, allowing the company to then determine whether or not they trigger any legal obligations.

The "I" acknowledges that there are state, federal and international laws relating to AI use cases that can be triggered and therefore need to be *identified*.

The "E" refers to the *establishment* of oversight and accountability for the scoping, determining of use cases, and identifying applicable laws. Often, but not always, this falls to the legal department, or the compliance and audit function.

The "L" suggests a *logging* or tracking of decisions that are made relating to the AI tool – for instance, what an acceptable use case might be; what the data sources are that are used to train or fine tune a model (which can relate to transparency obligations).

The "D" relates to *detecting* and responding to the changing legal landscape. The landscape has shifted in the past few months, and will certainly be shifting again.

A company needs to find a consistent way to track and update its compliance efforts to reflect any additional, or even reduced, obligations.

The SHIELD guidelines are flexible and assume a changing regulatory landscape. For the moment, companies have a smorgasbord of requirements that they need to fulfill, domestically and internationally.

It is a challenging but tremendously exciting time–no lawyer working in this area can claim a routinized practice.