JENNER & BLOCK

Takeaways from the White House's Framework for Artificial Intelligence

Client Alerts

March 26, 2026
By: Aaron R. Cooper, Will Weaver, Caroline Cease, Ashley Callen, Nikita Lalwani, Krister Rasmussen, Justin Iannacone

Overview

On March 20, 2026, the White House released a *National Policy Framework for Artificial Intelligence*, briefly recommending a set of legislative priorities for Congress across seven subject areas to "win[] the AI race." The framework represents the clearest statement to date of the Administration's ambitions for congressional action and offers a sense of where legislative engagement will likely focus over the coming year, including on preemption, child safety, and scaling infrastructure. But it is also short on details, surfaces competing policy ideas, and leaves potential tradeoffs unresolved—and a great deal of legislative work will be needed to turn any of these recommendations into law. Companies developing, deploying, or using AI should take note of the key principles of the framework and consider opportunities for advocacy and engagement, even as they continue to establish governance mechanisms to comply with state laws that have and will soon take effect. In the interim, federal AI policy is likely to continue to be driven by executive branch actions under existing authorities, including with respect to procurement and national security.

What the White House's Legislative AI Priorities Mean for the AI Stack

The framework addresses seven subjects: (1) protecting children and empowering parents; (2) safeguarding and strengthening American communities; (3) respecting intellectual property rights; (4) preventing censorship and protecting free speech; (5) enabling innovation and ensuring American AI dominance; (6) workforce and education; and (7) establishing a federal framework and preempting state AI laws.

Protecting Children and Empowering Parents. The framework identifies specific requirements for AI platforms and services likely to be accessed by minors, including age-assurance mechanisms (such as parental attestation), parental controls, and features to reduce risks of sexual exploitation and self-harm. Deployers in consumer-facing sectors should begin assessing whether their products meet these anticipated standards and tracking ongoing state legislative proposals in anticipation of

future regulation. Notably, although the framework calls for preemption for AI laws generally, in the child safety section it explicitly states that "Congress should ensure that it does not preempt states from enforcing their own generally applicable laws protecting children."

National Security and Economic Support for AI Scaling. Responding to ongoing concerns over energy affordability, the Administration calls on Congress to ease the regulatory and energy burdens of data-center construction so that AI developers can procure the infrastructure their models need without driving up consumer energy prices. The framework also urges Congress to provide grants, tax incentives, and technical assistance programs to support wider AI deployment in small businesses and across American industry. These initiatives aim to generate benefits for AI developers seeking to scale their capacity and their user base without impacting affordability, but whether that is a realistic outcome remains to be seen.

Further, against the backdrop of ongoing geopolitical competition over frontier AI leadership and recent reports of distillation attacks against US models, the framework also calls for defense and intelligence community agencies to develop sufficient technical capacity to assess frontier AI capabilities, and to consult directly with frontier AI developers as part of that process. Labs at the frontier of AI development should anticipate an increased government interest in direct engagement, including potential requests for information about model capabilities. This effort may build on current private sector engagements undertaken by the Center for AI Standards and Innovation, which has also included evaluations of models developed by China-based AI companies.

Congress is also asked to strengthen law enforcement tools to combat AI-enabled fraud and impersonation scams, particularly those targeting seniors. Deployers whose platforms could be used for such purposes should evaluate and consider strengthening existing safeguards.

Intellectual Property. The framework articulates the Administration's position on AI training and copyright, affirming for the first time in an official government publication the Administration's view that training on copyrighted material does not violate copyright law, while acknowledging that the issue remains contested and that courts should be allowed to resolve it. The Administration recommends that Congress not legislate on this question while litigation is ongoing. The framework also supports potential collective licensing frameworks for rights holders and calls for federal protections against unauthorized use of AI-generated digital replicas of individuals' voices and likenesses, with First Amendment carve-outs for parody, satire, and news reporting (similar to the federal NO FAKES bill introduced earlier this Congress).

Content Moderation and Free Speech. The framework's free speech recommendations are directed primarily at preventing government from forcing AI providers to alter content for partisan or ideological reasons. Developers and deployers should be cognizant that this framing signals Administration skepticism of content moderation practices perceived as ideologically motivated. Notably, however, the framework does not identify any objective baseline by which ideological

neutrality would be measured, further complicating this recommendation on a policy issue already fraught with First Amendment implications.

"American AI Dominance." The framework makes broad recommendations designed to ensure that the US "lead[s] the world in AI." It explicitly recommends against creating any new federal agency dedicated to AI, instead directing that AI regulation flow through existing sector-specific agencies and industry-led standards. It also supports establishing regulatory sandboxes for AI applications and making federal datasets available in AI-ready formats for model training. These are potentially significant benefits for developers, particularly those working on applications in regulated sectors. Sandbox proposals have also emerged in Congress in recent months: Senator Cruz (R-TX), for instance, has introduced one such proposal that would offer two-year regulatory waivers to AI developers (renewable up to four times).

Federal Preemption of State AI Laws. Perhaps the most consequential recommendation is the call for Congress to preempt state AI laws that impose "undue burdens," which echoes prior Administration efforts to establish a moratorium on state AI laws. Specifically, the framework recommends that states "should not be permitted to regulate AI development," proposing instead a single national standard. Yet unlike prior proposals, the framework does not call for complete preemption. Under the recommendations, states would retain traditional authority to enforce generally applicable laws (including consumer protection, fraud, and child safety laws) against AI developers and users, govern a state's own AI procurement and use, and regulate the siting of AI infrastructure.

Overall, the framework leaves considerable uncertainty over where Congress might draw the line between permissible and impermissible state regulations of AI. It also cautions against states penalizing developers for third-party misuse of their models, opening the door to a significant potential liability shield that resembles the statutory defenses protecting gun manufacturers (under the 2005 Protection of Lawful Commerce in Arms Act) or social media platforms (under Section 230 of the Communications Decency Act).

What the Framework Leaves Open

Specific Implementation Guidance. The framework makes suggestions for *what* Congress should seek to do in general terms but says little about *how*. For example, it directs Congress to require AI platforms and services likely to be accessed by minors to "implement features that reduce the risks of sexual exploitation and self-harm to minors," but does not specify what these features ought to be. Similarly, the framework advocates for a "minimally burdensome national standard" but is silent as to what specific standard Congress ought to adopt. Much of the actual legwork will therefore need to be undertaken by Congress, but as further laid out below, Congress is divided on many of these issues and may be unwilling or unable to take action.

Labor Market Disruption. The framework's priorities do not prominently address the possibility that the proliferation of AI could lead to widespread unemployment or labor-market disruption, as many economists, policymakers, and industry players have predicted. Instead, the framework appears squarely focused on a future in which AI augments rather than replaces human labor, calling for measures to accelerate the AI rollout into the workforce and the creation of new jobs in an AI-powered economy.

Liability and Risk. The framework does not devote significant attention to questions of how to manage risks of harm from AI that acts against or without human authority, which is another area of danger that AI developers and critics alike have highlighted. While the framework is sensitive to the possibilities of human misuse of AI, it does not grapple in a detailed manner with the risk that agentic AI could act with limited human control and oversight. And it says little on the question of liability for harms caused by AI, except to advise against the setting of liability rules that could give rise to excessive litigation.

Looking Ahead

The framework is a legislative wish list, not proposed statutory text. Congress will determine whether and how much of it becomes reality, and many lawmakers are opposed to broad efforts to preempt state regulation of AI. Senator Marsha Blackburn (R-TN), who helped sink congressional preemption efforts last summer, has declined to endorse the White House's proposal. Across the aisle, Rep. Josh Gottheimer (D-NJ), co-chair of his party's AI commission, called the framework a "half-measure that falls short of what's necessary for 'Smart AI' regulation," adding that preemption works only "if federal law effectively replaces what states have built with a standard that is truly comprehensive and protects Americans."

Of course, any congressional preemption efforts are also likely to face blowback from the states. On March 3, for example, more than 50 state Republican lawmakers signed on to a letter urging the White House to stop efforts to block state AI laws, declaring their belief that "state-led efforts are fully consistent with conservative principles and with [the Administration's] stated goals of promoting human flourishing while accelerating innovation."

That said, the framework carries significant weight as a signal of Administration priorities, and many of the recommendations—particularly on preemption, child safety, and the rejection of a new AI regulator—align with positions that have gained traction in recent congressional discussions. Ultimately, however, it remains unclear whether any of these policies can be put to paper in a manner that garners enough congressional support to become law, or if they will merely serve as a vehicle for policy alignment by like-minded officials at state and federal levels.

Companies should monitor legislative developments closely and consider engaging with Members and staffers, even as they continue to work with state governments to abide by state regulatory

frameworks that remain in effect. Amid regulatory uncertainty, companies should develop compliance programs and strategies that can adapt to state requirements as well as any potential federal standards, all while ensuring their technology is safe, harmless, and compliant with existing legal frameworks.

Related Attorneys

Aaron R. Cooper
Partner
acooper@jenner.com
+1 202 637 6333

Will Weaver
Partner
wweaver@jenner.com
+1 202 639 6870

Caroline Cease
Partner
ccease@jenner.com
+1 202 639 6056

Ashley Callen
Partner
acallen@jenner.com
+1 202 639 6000

Nikita Lalwani
Associate
nlalwani@jenner.com
+1 202 639 6021

Krister Rasmussen
Associate
krasmussen@jenner.com
+1 202 639 3844

Justin Iannacone
Associate
jiannacone@jenner.com
+1 415 293 5949

Related Capabilities

Congressional Investigations

Critical and Emerging Technologies

Government Controversies and Public Policy Litigation

Stay Informed →