New American

Written by **Veronika Kyrylenko** on March 24, 2026

Trump, Blackburn Push to Federalize AI Control

AP Images
Marsha Blackburn

The Trump administration and its allies in Congress are moving to define the rules of the digital future, with consequences that could extend far beyond artificial intelligence (AI).

Last week, the White House released a national AI legislative framework, while Senator Marsha Blackburn (R-Tenn.) introduced a sweeping, 291-page companion bill to codify it into law. Together, they mark the most aggressive federal push yet to define how Americans access, use, and build AI systems.

Supporters argue the country needs a single national standard to compete with China and rein in Big Tech. The language is polished and ambitious. It promises to protect children, safeguard free speech, support creators, spur innovation, empower communities, and prepare Americans for an "AI-driven economy."

Critics see something else: Identity-gated access, continuous monitoring, traceable content, and federally managed AI development.

At the center of the debate is a simple question: Who controls access to AI, and at what cost?

One National Framework

At the core of the Trump administration's AI push is a single premise: Centralization of AI regulation.

The White House states it plainly:

> Importantly, this framework can succeed only if it is applied uniformly across the United States. A patchwork of conflicting state laws would undermine American innovation and our ability to lead in the global AI race.

Blackburn's bill sharpens the point. Its title is telling:

> The Republic Unifying Meritocratic Performance Advancing Machine Intelligence by Eliminating Regulatory Interstate Chaos Across American Industry Act (TRUMP AMERICA AI Act).

In other words, when states regulate AI, it is, in the senator's telling, "chaos." When Washington does it, it a "unifying" order.

"The Federal government is uniquely positioned to set a consistent national policy," the White House adds.

The effect is sweeping. A single federal framework would override emerging state laws. States such as California and New York have already begun shaping AI rules. Under this model, those efforts would be sidelined.

Blackburn's bill turns that vision into structure. It consolidates authority across safety, liability, and enforcement. It expands federal oversight and delegates rulemaking authority to agencies such as the Federal Trade Commission (FTC).

Other provisions reinforce the shift. The Department of Energy (DOE) gains authority to evaluate advanced systems, centralizing access to data and infrastructure.

Age Verification and the Identity Layer

The most controversial element centers on identity.

The framework calls for age verification across AI platforms. In practice, that means users must prove who they are before accessing certain systems.

The White House states it directly in its legislative recommendations:

> Congress should establish commercially reasonable, privacy protective, age-assurance requirements (such as parental attestation) for AI platforms and services likely to be accessed by minors.

That language sounds flexible. The enforcement mechanism is not.

The related legislation shows how this would work. The GUARD Act (S. 3062), one of 17 measures bundled into Blackburn's bill, requires that every user of an AI chatbot create an account before access. Every account must be age-verified. The bill defines acceptable methods as "a government-issued identification," or an equivalent commercial system.

The platforms are allowed to "contract with a third party" to verify a user's age. In practice, that often means data brokers, companies that specialize in collecting, aggregating, and selling personal information.

The flow is simple: You upload your ID, brokers verify it. They now have your ID linked to your use of the platform. The AI company also knows who the user is — and can be asked to share this with the government.

Blackburn's proposal goes further, potentially extending the scope of identification beyond AI platforms. It reaches into the devices themselves. Section 417 mandates a federal study on "the benefits of creating a device or operating system level age verification system." The study must also examine what data would need to be collected and whether hardware or software changes would be required, including for devices already in use.

"Duty of Care" and Surveillance

Another pillar of the framework is the promise of safety.

Blackburn's bill imposes a "duty of care" on AI developers and platforms. Under Section 101, developers must "exercise reasonable care" to prevent and mitigate "reasonably foreseeable" harms

tied to the design and operation of their systems. The FTC would oversee compliance.

Section 412 requires companies to ensure their features do not contribute to harms such as suicidal behavior, eating disorders, anxiety, compulsive use, harassment, sexual exploitation, substance abuse, and financial harm.

The operational implication is clear. To prevent harm, platforms must detect it. To detect it, they must observe user behavior. And to prove compliance, they must show that monitoring is active and effective.

In other words, that structure risks transforming duty of care into a system of continuous oversight, particularly over minors' online activity.

The concern is not abstract. Systems built to track, verify, and monitor behavior at scale create sensitive pools of data. Identity-linked behavioral data, especially involving children, becomes a high-value target for misuse, breach, or exploitation.

Liability, Censorship, and Bias

Besides the cynical pitch of "protecting children," proponents highlight what they frame as clear wins: repealing Section 230 of the Communications Act, curbing DEI influence, and promoting free speech online. But all of those claims are questionable, at best.

Start with Section 230. Today, it does two things. It shields platforms from liability for user-generated content, and it allows them to moderate in good faith. Repeal is presented as a way to hold Big Tech accountable for its "woke" censorship. In practice, it strips both protections at once, so every platform that hosts user content becomes exposed to constant litigation. But that exposure does not fall evenly. Large platforms can absorb it. Smaller platforms cannot. As a result, the very alternatives built to challenge Big Tech become the most vulnerable.

The anti-bias and anti-DEI provisions in Title VIII and Title XVI follow a similar pattern. They promise neutrality — which actually is not self-executing. It depends on who defines it and who enforces it, reflecting the priorities of the administration in power.

Then there is content provenance. Title XIV requires persistent, machine-readable markers on AI-generated content. The stated goal is to combat deepfakes and "protect artistic content." The structural effect is broader: It creates a traceable chain of origin for AI-assisted speech.

The Program

The bill's core enforcement mechanism is called the Advanced Artificial Intelligence Evaluation Program, established under Section 603 within the DOE. It must be created within 90 days of enactment.

On paper, it is a safety initiative. The program conducts testing of advanced AI systems, including adversarial "red team" exercises designed to simulate real-world attacks. It evaluates risks, produces reports, and recommends mitigation strategies.

The program is also tasked with "collect[ing] data on the likelihood of adverse AI incidents" and using that data to "inform the creation of evidence-based standards, regulatory options, guidelines, and governance mechanisms." It does not just test systems — it helps define how they will be governed.

It also introduces classified oversight. The program may conduct "classified, independent third-party assessments" and "blind model evaluations," placing key parts of the process outside public view.

The scope expands sharply in its forward-looking requirements. The program must provide "comprehensive evaluations" on whether AI systems could "exceed human oversight," approach "artificial superintelligence," threaten economic competition, "undermine civil liberties," or pose "existential risks to humanity."

It must also analyze system behaviors such as "weaponization potential," "self-replication capabilities," "scheming behaviors," and "autonomous decisionmaking."

Those findings then translate into policy. The program is required to recommend "standards, certification procedures, licensing requirements, and regulatory oversight structures."

It goes further still. The program must outline "automated and continuous monitoring" of AI hardware usage, compute inputs, and cloud deployments. In effect, AI systems would operate under continuous, automated oversight, likely enforced by the same class of technologies they are built on.

Federal Power and Control of AI Systems

Participation is mandatory. Section 602 provides that developers of advanced AI systems must enroll and comply to operate. Noncompliance can trigger penalties of up to $1,000,000 per day.

To meet that requirement, developers must provide the government, on request, with "materials and information necessary" to run the program. The scope is expansive. It includes the underlying source code, training data, model weights, the interface engine, and detailed information about system design and operation.

The language is explicit. "No person may deploy an advanced artificial intelligence system for use in interstate or foreign commerce unless" they are in compliance.

That level of compelled access raises immediate concerns. The same authority that tests AI can define the rules, enforce them, and decide who is allowed to operate. What begins as evaluation becomes governance.

And governance, in this framework, is federal. Pitched in noble terms, it concentrates control over a highly consequential technology inside a single regulatory apparatus with well-known limits in transparency, accountability, and restraint.

Related article:

Trump Set to Centralize AI Policy as Federal AI Mission Expands