# Battle for AI Governance: White House's Plan to Centralize AI Regulation and States' Continuous Opposition

**Related Professionals**

Christopher L. Ingram

Christopher A. LaRocco

Celina J. Needle

**Related Services**

Data Strategy, Privacy and Security

**CLIENT ALERT** | 4.28.2026

The fight over who will shape artificial intelligence (AI) regulation in the United States is becoming sharper. On one side, the Trump Administration is pressing for a single, national framework that limits fragmented state-by-state rules. On the other, states like California, Colorado, Utah, and Texas who have enacted and continue to enact AI-related laws are moving ahead with their own compliance regimes. For organizations leveraging AI, including those entrusting their data to such organizations, the fight between federal and state regulations includes profound implications for data privacy as businesses and consumers stand between the crossfires.

## Federal Takeover: Goodbye State Patchwork?

On December 11, 2025, President Trump signed an executive order on AI, marking a pivotal shift in the regulatory landscape as the White House attempts to centralize AI regulation. The executive order's directive is clear: unify AI oversight at the federal level and reduce patchwork state regulations. Its central provision directs federal agencies to identify and challenge state AI laws deemed inconsistent with national policy.

President Trump tasked the Attorney General with coordinating litigation efforts against state measures that impose what the administration characterizes as innovation-limiting requirements, and in January 2026 the Attorney General announced the AI litigation task force, as directed by the executive order. Moreover, the order also allows federal funding and infrastructure support to be conditioned on state alignment with national AI policy.

Following the December executive order, on March 20, 2026, the White House released a four-page blueprint directing Congress to adopt a unified federal approach to AI governance. The framework includes six broad objectives: (1) protecting children online, (2) safeguarding against AI-related harms, (3) respecting intellectual property rights, (4) preventing AI-driven censorship, (5) promoting innovation, and (6) developing an AI-ready workforce. Most importantly, the framework

calls for federal preemption of state AI laws, arguing against "patchwork" state laws as an obstacle to innovation. However, the framework also leaves wide regulatory gaps regarding bias standards, adult data privacy protections, and transparency mandates, possibly allowing for state and local governance for such regulations.

## States' Response to the Federal Effort

States have begun responding more directly to the executive order, both through continued legislative activity and public statements from state officials. Notably, several state-level AI statutes have taken effect or are scheduled to take effect in 2026. This includes California's AI Transparency Act and Texas's Responsible Artificial Intelligence Governance Act, both of which incorporate privacy focused provisions and impose disclosure and governance requirements related to transparency, automated decision making and how personal data can be used to train or operate AI systems. Colorado's comprehensive AI legislation is also scheduled to take effect on June 30, 2026, further expanding state-level regulation of high-risk AI systems.

In parallel, there is no indication that state legislative activity is slowing in response to the federal initiative. Multiple states continue to advance AI-related bills toward enactment, including Washington, where several AI-related measures have progressed; Florida, where proposed legislation seeks to establish AI-related consumer rights; Virginia, where legislation addressing the use of AI in mental health applications has advanced; and Utah, where amendments addressing AI transparency requirements have moved through the legislative process. These developments reflect sustained momentum at the state level despite the Trump Administration's emphasis on federal coordination. By asserting federal primacy, privacy protections embedded in state frameworks could be narrowed or displaced. While this may reduce compliance fragmentation, a federal overhaul may also eliminate specific data-handling standards that currently guide AI governance practices.

## Navigating Legal Uncertainty: Compliance is Still Key

The executive order does ***not*** create a comprehensive federal AI privacy law. Instead, it directs federal agencies such as the Department of Commerce and the Federal Trade Commission to evaluate existing regulatory requirements and consider whether federal standards should replace or supersede state rules. Thus, much remains uncertain.

It is important not to assume federal rules will be lighter or less stringent than current state regulations. While the order emphasizes minimizing regulatory burdens rather than expanding consumer data rights, the ultimate privacy impact will depend on how agencies implement these directives. For now, state privacy statutes remain operative. States may contest federal primacy, leading to constitutional challenges over preemption and states' rights. Businesses must continue to comply with existing state requirements unless and until federal preemption issue is clarified.

Recent developments also suggest that litigation and enforcement activity involving AI is picking up. In March 2026, the federal government took positions in litigation involving AI companies in areas such as national security and supply chain risk, signaling a willingness to engage in disputes involving the regulation and use of AI technologies. These developments, together with the establishment of the Department of Justice's AI Litigation Task Force, indicate that judicial proceedings may play a significant

role in shaping the contours of AI regulation in the near term.

## Trust, Reputation, and Sector-Specific Obligations

Privacy risks exist even if federal policy eventually results in fewer regulatory obligations. Reputational harm can arise if companies are seen as exploiting regulatory gaps. Stakeholders, including investors and strategic partners, are factoring privacy and data governance into assessments for organizational risk and value. Likewise, the EU's General Data Protection Regulation (GDPR) remains at the forefront of international privacy regimes.

## The Broader Privacy Landscape

The executive order and White House framework signal a shift toward centralized federal control over AI regulation. The immediate result, however, is legal uncertainty rather than immediate deregulation. Existing state privacy and AI laws remain operative, and sector-specific federal privacy statutes continue to apply. For businesses, it is prudent not to treat the executive order or the framework as a green light for relaxed data practices. Organizations deploying AI systems should continue to maintain compliant data governance, conduct internal risk assessments, and monitor evolving state and federal guidelines.