The Inconsistent State of U.S. Tech Policy: How Washington is Fighting Itself, the States, and the World on AI Safety

State-level leadership in online safety is currently facing converging pressures from two distinct federal directions. This renewed debate over preemption–the constitutional principle by which federal law supersedes state law–places the future of digital consumer protection at a critical juncture. Ideally, federal law should set a baseline floor of online safety protections that states can build on top of, within reason. However, absent effective federal action, states should be allowed to pass policies that keep their residents safe online.

Broad Statutory Preemption and Conditional Funding as Deregulation

Congress is considering several child safety and privacy measures that utilize an expansive "relates to" preemption standard. From a statutory interpretation perspective, this language is significant. Unlike narrower standards that only preempt state laws that strictly conflict with federal rules, a "relates to" standard could broadly displace any state legislation touching on the same subject matter. Such a provision could effectively nullify robust state-level protections, replacing them with a federal standard that may be weaker or less agile in addressing emerging harms. This is most actively concerning when it comes to AI, as states are passing laws to regulate this new and expanding technology while Congress does not have a clear approach, meaning that consumer safety relies on which state you live in, or industry self-regulation and voluntary commitments.

Simultaneously, the Executive Branch is signaling a shift in how federal leverage is applied to AI policy. In December 2025, President Trump signed an Executive Order to prevent states from implementing strict AI regulations, creating a task force to challenge state laws and even threatening federal broadband (BEAD) grants if states don't comply. This approach utilizes fiscal federalism not to encourage higher

standards, but to incentivize deregulation. By tying critical infrastructure funding to regulatory inaction, this policy would effectively penalize states that attempt to legislate on AI safety, forcing a choice between digital access and digital oversight.

If Congress Can't Provide a Comprehensive National AI Policy, Why Should States Wait?

A timely example of this regulatory tension is Florida's AI Bill of Rights. Spearheaded by Governor Ron DeSantis and filed by State Senator Tom Leek in December 2025, it has become a case study in the collision between state regulatory ambition and federal preemption threats. The Trump administration's AI Litigation Council has signaled intent to challenge "onerous" state AI laws. Florida's legislation, with its parental consent mandates, data protection requirements, and disclosure obligations, provides a concrete test of where federal preemption authority begins and state regulatory powers end.

Several provisions in Florida's bill face significant preemption vulnerability. The requirement that AI platforms obtain parental consent before minors access companion chatbots likely implicates federal authority over interstate commerce and children's online protection. The Children's Online Privacy Protection Act (COPPA) already establishes federal standards for collecting information from children under thirteen. Florida's broader age assurance requirement could conflict with federal frameworks if the FTC or Congress establishes different verification standards. More critically, implementing state-specific parental consent systems for nationally distributed AI platforms creates exactly the compliance fragmentation that preemption principles aim to prevent.

The bill's prohibition on government contracts with AI firms tied to "foreign countries of concern" similarly encroaches on federal domain. Foreign policy and national security restrictions traditionally fall under exclusive federal authority and states that have tried to regulate under the basis of national security have faced legal injunctions. While states can make procurement decisions, a blanket ban based on foreign connections intersects uncomfortably with federal trade oversight, sanction regimes, and diplomatic relations. If federal agencies determine that certain Chinese or Russian AI technologies pose acceptable risks under specific conditions, Florida's categorical prohibition could directly conflict.

Florida's data protection provisions, barring the sale of non-deidentified personal data and requiring disclosure of AI interactions, raise different preemption questions. Privacy regulation has historically been a mixed state-federal domain. States from California to Virginia have passed comprehensive privacy laws without federal interference. However, if Congress passes comprehensive federal privacy legislation, Florida's AI-specific data rules could be preempted depending on whether federal law sets a ceiling or a floor for state action.

Existing national AI frameworks are geared toward maintaining economic competitiveness and addressing national security concerns, resource allocation, and other macro-level priorities. These frameworks typically do not center children's digital safety. Since states are closer to the residents affected by risks posed by digital platforms and AI tools, they bear some responsibility to address these harms directly.

While some states have pursued extreme measures, such as outright social media bans, **the more productive approach involves empowering states to regulate how platforms operate within their borders to prevent documented risks.** The available national AI framework does not address critical nuances like age assurance, algorithmic feeds, companion chatbots, and data privacy protections, precisely the issues states have incorporated into their digital safety policies.

The recent introduction of a House companion bill for the Kids Off Social Media Act (KOSMA) is one option for resolving federal-state tension by establishing a federal floor. The bill aims to address age restrictions, restrict algorithms, establish school requirements, and data privacy protections, mirroring elements of Australia's approach. However, blanket bans do not always solve the problems they target, especially on platforms that have proven beneficial and productive for young people. Policymakers must first carefully consider what constitutes "social media," define the specific risks from which children need protection, and then develop pragmatic solutions that safeguard young people from digital harms without inadvertently limiting their educational opportunities and social development.

KOSA vs. Trump's AI Plan

We are currently witnessing a collision between two fundamentally incompatible visions for the internet. On one side, the Trump administration is advancing an AI Manhattan Project (Genesis Mission) focused on deregulation, energy dominance, and rapid deployment to secure an advantage over China. This executive

vision views safety guardrails essentially as speed bumps, and it seeks to preempt state laws primarily to remove friction for industry. On the other side, Congress is pushing forward with the Kids Online Safety Act (KOSA), which is built on the opposite premise: that the digital ecosystem is already too dangerous and requires strict new obligations. The Senate version of KOSA imposes a "duty of care" and mandates safety-by-design features, narrowly preempting state laws to establish a higher, uniform standard of protection.

Both the White House and Congress are attempting to seize control of the regulatory landscape, but they are pulling in opposite directions. The administration wants to use federal power to slash the safety net to "unleash" AI, while many in Congress want to use federal power to weave a tighter net to protect children. The difference feels even more stark when realizing the safety efforts are concentrated on solving yesterday's online harms (social media) while the deregulation efforts are to prevent addressing tomorrow's online risks (AI). We are seeing a willingness to mortgage the future to secure immediate market dominance. Is the race for American AI supremacy truly worth the cost? Are we willing to delay the critical work of designing a safer online world for our children simply to win the AI race? Why trade the benefits of passing legislation that creates safety protections on social media platforms for *preventing* meaningful safety regulations on AI?

Export American AI *and* "Deregulation"?

This aggressive deregulatory stance is extended to the desire for global leadership. The current administration views AI regulation as a strategic vulnerability in the AI race against China. This is leading to an international dialogue in which the U.S. is now actively pressuring allies to pump the brakes on their own safety frameworks. Sriram Krishnan, White House senior policy advisor on AI, used the AI Impact Summit in New Delhi to criticise the EU AI Act as harmful to innovation and reiterate the U.S.' opposition to the law.

This echoes remarks at CES in Las Vegas from William Kimmitt, head of the Commerce Department's International Trade Administration, who put it bluntly that the U.S. does not want the rest of the world to follow the EU's AI standards. He signaled that the U.S. is prepared to push trading partners to delay their regulatory processes, using tariffs on steel and aluminum and access to the U.S. market itself as leverage.

This coercive approach stands in sharp contrast to the cooperative model FOSI has long championed. We have consistently urged countries to work together on regulating the internet and learn from one another in the process. For example, the UK passed its Age Appropriate Design Code (AADC) in 2020 and has years of practical experience regarding the pros and cons of online safety regulation. It would be myopic to treat such experience and frameworks as economic threats. Instead, it is prudent to treat them as valuable case studies in how to build a safer internet.

The Path Forward For Online Safety

The reality is that this is a difficult balance. There is not a one size fits all solution. It's hard to strike the right balance of innovation and regulation, of harmonization across jurisdictions, and across borders and languages and cultures. A few possible policies include:

- Enact a federal data privacy law to ensure all online users have protections for their personal data. A data privacy floor at the federal level should leave room for states with more comprehensive approaches.
- Allow some flexibility for states to thoughtfully regulate specific harms in online safety, such as efforts to enhance safety protections for minors interacting with chatbots. Harmonization, however, is key to ensure all minor users across the country are kept safe and industry can comply with emerging laws.
- Thoughtfully incorporate age assurance mechanisms in online safety policies intended to protect minors. This includes certain AI chatbot or companion products, risk-based proportional protections for features such as live chatting and live streaming, and algorithmic personalization options. Age assurance will not solve everything, but it can be a key step in improving kids' safety online. A complete moratorium on AI regulations or "relates to" preemption language could prevent states from utilizing this tool to create age appropriate online experiences. Read FOSI's updated report, Balancing Safety and Privacy: A Proportionate Age Assurance Approach, to learn more about FOSI's age assurance principles.

Ultimately, it is better to have comprehensive online safety protections at the federal level. **But if Congress and the administration cannot act, states should not**

be prevented from implementing thoughtful and nuanced policies. We want to build a digital world that we are actually proud to hand over to the next generation.