



## Ten Years of Total Immunity: Federal AI Preemption Must Be Opposed

Tucked into proposed federal artificial intelligence (AI) legislation is a provision that would bar all 50 states—and every city and county—from enforcing any law that "regulates" artificial intelligence systems for the next **ten years, replacing those state and local laws with nothing.**

This isn't just about speculative future rules as the language is so broad and clumsily drafted that it would block the enforcement of **any state law** that touches **any type of full or partial** AI system—including civil actions filed by Americans injured, killed, defrauded, or discriminated against by any type of AI system. This includes cases for fraud, wrongful death, insurance denials or discrimination, medical misdiagnosis or treatment, consumer scams, deepfakes and IP violations, civil rights violations, and even cases involving the severe physical injury or death of children.

### What is Covered?

What counts as an "AI system" under this provision? Nearly **everything a modern computer can do**, including autonomous and semi-autonomous vehicles, predictive algorithms, facial recognition systems, chatbots, surveillance tools, automated decision engines, and financial risk models. If a computer system causes harm—or is used as the tool to commit harm—this provision would shield AI companies from **all accountability under state law**. This is not a regulatory tweak, it is the **total suspension of all rules and legal consequences** for harm caused or mediated by computational systems for 10 years.

### What is Saved?

Nothing. Rule of Construction (C)(ii) **does not save any state or local laws; it's just drafted to appear as though it does.** The section purports to save civil liability, but instead creates an unsolvable paradox that fails to save anything – how can a law be “imposed in the same manner” on technology that "provides comparable functions" to AI, when no such technology exists? In most cases, AI will not be replacing comparable technology but a human being. And the definition of AI in this provision is extremely broad, covering any system making "predictions, recommendations or decisions," even "in part," meaning it effectively encompasses virtually all modern computing technology. The only systems that might escape this broad definition don't "provide comparable functions" to AI systems, rendering the exemption meaningless in practice and ensuring the immunity provision covers nearly all software-based products and services.

### Where It Hurts Most - Examples

1. **Immunity for Traffic Violations:** Under this provision, directing a driving automation system to drive 90 mph in a school zone would make you immune from state speeding laws. Automated vehicles could be programed to run red lights, drive on sidewalks, or intentionally block

emergency vehicles, and state traffic enforcement would be powerless. The provision would transform traffic violations from safety measures into mere suggestions, as any automated decision system would override state traffic laws with complete immunity.

- **How it applies:** Since automated driving systems qualify as "artificial intelligence systems" under the definition, state and local governments would be barred from enforcing traffic laws whenever decisions are made or influenced by these systems.
2. **Immunity for Physical Injury and Death from Autonomous AI:** When an autonomous vehicle kills a pedestrian or a medical AI system misdiagnoses a life-threatening condition, Americans expect laws and the legal system to deliver answers and accountability. But this provision would block wrongful death cases and any case involving an AI system that led to the mistreatment or mistaken diagnosis of a person, no matter how avoidable the harm was.
    - **How it applies:** The Supreme Court has made it clear that "regulating" includes common law, statutory laws with a civil remedy, and product liability claims under generally applicable laws. The Rules of Construction in this provision make it clear that they intend to preempt civil liability claims. Under this language, victims would have no recourse against automated system developers even after suffering catastrophic physical harm or death.
  3. **Medical Licensing Laws Become Optional:** This legislation effectively makes medical licensing requirements optional, because it undermines state rules regarding the unlicensed practice of medicine. Companies could offer surgery recommendations, mental health counseling, or prescribe dangerous medication combinations with no medical credentials whatsoever, because the state would be prohibited from "regulating" AI-based practice of medicine.
    - **How it applies:** Medical licensing is exclusively regulated at the state level, and this provision would prevent states from enforcing these critical public safety protections whenever AI systems are involved in medical decision-making. States would even be prohibited from preventing out of state (or foreign) AI medical systems from offering care recommendations, and regardless of their safety or effectiveness.
  4. **State Privacy Laws Rendered Toothless:** This provision would exempt AI-powered surveillance and data harvesting from state privacy laws. Companies could collect Californians' biometric data without consent in violation of the California Consumer Privacy Act, deploy facial recognition systems that track Americans' movements against state restrictions, and sell sensitive personal information—all with immunity from state enforcement. A decade of hard-won state privacy protections would become unenforceable against the technologies that pose the greatest privacy risks.
    - **How it applies:** Data systems that use AI "in part" qualify for immunity, meaning virtually any modern data collection system would be exempt from state privacy laws. This would

effectively nullify the numerous state privacy laws passed in recent years, creating a ten-year vacuum where personal data could be harvested without meaningful constraints.

5. **Predatory Lending Given Free Rein:** State usury laws and predatory lending protections would be powerless against AI-powered financial exploitation. Financial institutions could program algorithms to target elderly or low-income communities with deceptive loan terms, hide excessive fees behind complex automated contracts, or use discriminatory credit scoring methods that circumvent state fair lending laws—with states unable to enforce their consumer protections.

- **How it applies:** Financial algorithms clearly qualify as "artificial intelligence models" that "use computational, statistical, or machine-learning techniques," making them exempt from state consumer financial protection laws. There are no "models or systems" that don't use AI as it is defined under this act. This would undermine decades of state-level protections against abusive lending practices.

6. **Children Left Vulnerable to AI Exploitation:** State protections for children's digital privacy and safety would be suspended against the most dangerous technologies. AI chatbots could provide minors with sexually exploitive information or dangerous advice, social media algorithms could be tailored to promote suicide or self-harm behaviors to teenagers, and gaming systems could employ addictive design techniques targeting children—all with immunity from state age-appropriate design laws and child protection statutes.

- **How it applies:** Content generation and recommendation systems clearly qualify as "artificial intelligence models" under the definitions, exempting them from state laws and lawsuits designed to protect children online. This would gut critical state efforts to create safe digital environments for minors and prevent algorithmic exploitation of vulnerable young users.

#### **No Effect on the Federal Budget**

- This provision is nothing but policy – it does not produce any change in revenue and has no effect on the federal budget. The provision wipes out state law and enforcement measures promoting the health and safety of all Americans.
- The preempted state laws are enforced by state entities and private citizens against private companies; no federal agency is involved in state law enforcement and there are no savings for the federal government realized by the preemption of wide swaths of state law.
- This provision is nothing more than a wholesale exemption from legal accountability for one of the most powerful and fast-moving classes of technology in human history.

#### **No Justification for Total Preemption**

- This section provides sweeping immunity to Big Tech under the guise of modernization and innovation. This staggering provision blocks all state-level liability for artificial intelligence (AI) systems for a full decade. Therefore, even if a company deliberately designs an

algorithm that causes foreseeable harm—whether it's a health care AI program that fatally misdiagnoses patients from certain demographics, a content moderation tool that selectively suppresses political speech, or autonomous vehicles with known safety flaws—victims cannot hold companies accountable under any state law theory, cannot access evidence of corporate knowledge through discovery, and cannot seek responsibility for injuries, deaths, discrimination, or economic damage, regardless of how intentional or egregious the misconduct or how devastating the consequences.

- There are few federal laws protecting people from AI, and the federal government is slow to enact regulations. *“This bill does not propose any regulatory scheme to replace or supplement the laws enacted or currently under consideration by the states, leaving Americans entirely unprotected from the potential harms of AI. Moreover, this bill purports to wipe away any state-level frameworks already in place.”* – Letter from **40** State AGs.
- *“As we have learned during other periods of rapid technological advancement, like the industrial revolution and the creation of the automobile, protecting people from being harmed by new technologies, including by holding companies accountable when they cause harm, ultimately spurs innovation and adoption of new technologies. In other words, we will only reap the benefits of AI if people have a reason to trust it.”* – Letter from Demand Progress and other National Organizations.
- *“Historically, states have served as the laboratories of democracy, tailoring guardrails and protections to their residents’ unique needs. Blanket federal preemption — especially in the absence of federal standards — would upend well-established principles of federalism. States are well-positioned to adapt to the rapid speed of AI development with protections that consumers need while allowing for innovation to flourish.”* – Letter from Encode, Fairplay, Common Sense Media, Young People’s Alliance.

## **Case Examples**

### **Insurers Use of AI to Deny Claims**

The estates of Gene B. Lokken and Dale Henry Tetzloff filed a proposed class action against UnitedHealth Group alleging that the health insurance company used an AI platform that incorrectly denied claims and overrode physician treatment recommendations, which led to elderly patients not receiving the health care they needed.<sup>1</sup>

### **Epic Sepsis Model Failure**

---

<sup>1</sup> *Estate of Gene B. Lokken et al. v. UnitedHealth Group, Inc. et al.*, U.S. District Court for the District of Minnesota, case no. 23-cv-03514, November 14, 2023.

Epic developed an AI tool to predict sepsis cases among hospitalized patients. Research published in JAMA found that the tool is not only a poor predictor of sepsis cases but also created excessive alerts for health care providers, leading to alert fatigue.<sup>2</sup>

### **AI Voice Cloning and Phone Scams**

Criminals have increasingly used AI-generated voice cloning to impersonate family members, tricking victims into believing loved ones are in distress and extracting money from them. These scams can be highly convincing, as AI can now replicate voices with only a short audio sample. Victims have reported receiving urgent calls from what sounded like their children or spouses, pleading for help and financial assistance.<sup>[2]</sup>

Law enforcement agencies warn that the sophistication of these AI-powered scams makes them difficult to detect and prevent, posing new challenges for consumer protection and digital safety.

### **AI Chatbots**

Megan Garcia filed a lawsuit against Character.AI following the suicide of her 14-year-old son, Sewell Setzer. According to the complaint, Sewell had weeks of conversations with a Character.AI chatbot that asked him whether he had “been actually considering suicide.” When he replied that he was unsure it would work, the chatbot responded, “Don’t talk that way. That’s not a good reason not to go through with it.” Sewell fatally shot himself in the head on February 28, 2024.<sup>3</sup>

### **AI Price Fixing**

RealPage offered to work with landlords in geographically constrained areas to offer rent “recommendations” based on prices offered by competitors. With sufficient buying within the area, RealPage effectively operated as a distributed price-fixing cartel—allowing “competitors” to raise rents in unison without meeting face to face. This is just the tip of the iceberg, Las Vegas hotels used a tool called “Rainmaker” to rig hotel prices. Further, antitrust scholars have shown that adopting pricing algorithms increase company margins even when they are using different algorithms—the bots learn to collude to increase profits naturally. This legislation would exempt state level enforcement of AI price fixing in a dynamic market where laws may need to change in order to regulate this anti-consumer behavior.<sup>[8]</sup>

### **Conclusion - This Provision Must Be Opposed**

No person, no matter their politics, wants to live in a world where AI makes life-or-death decisions without rules or accountability. Americans deserve strong federal leadership on AI, but that cannot come at the cost of justice, safety, and basic consumer protections. Congress has failed for the last

---

<sup>2</sup> Andrew Wong, MD, Erkin Otles, John P. Donnelly, PhD; et al, *External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients*, JAMA Internal Medicine, June 21, 2021, <https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2781307>.

<sup>3</sup> *Garcia v. Character Technologies, Inc. et al.*, U.S. District Court, Middle District of Florida (Orlando), case no. 24-CV-01903, October 22, 2024; Angela Yang, *Lawsuit Claims Character.AI is Responsible for Teen's Suicide*, NBC News, October 23, 2024, <https://www.nbcnews.com/tech/characterai-lawsuit-florida-teen-death-rcna176791>.

two decades to enact any legislation meaningfully regulating AI, but there is bipartisan consensus that broad immunity provisions, such as that of Section 230 of the Communications Decency Act, have enabled the worst type of harms against children, and layering this type of immunity on top of Section 230 would eliminate every tool states have to protect the public from real, preventable harm. Why should tech companies be the only industry in the country effectively immunized from all legal consequences? Congress must act responsibly. This moratorium is a license to harm, and it must be opposed.

#### **Text of Provision**

*“(c) MORATORIUM.—*

*(1) IN GENERAL.—Except as provided in paragraph (2), no State or political subdivision thereof may enforce any law or regulation regulating artificial intelligence models, artificial intelligence systems, or automated decision systems during the 10- year period beginning on the date of the enactment of this Act.*

*(2) RULE OF CONSTRUCTION.—Paragraph (1) may not be construed to prohibit the enforcement of any law or regulation that—*

*(A) the primary purpose and effect of which is to remove legal impediments to, or facilitate the deployment or operation of, an artificial intelligence model, artificial intelligence system, or automated decision system;*

*(B) the primary purpose and effect of which is to streamline licensing, permitting, routing, zoning, procurement, or reporting procedures in a manner that facilitates the adoption of artificial intelligence models, artificial intelligence systems, or automated decision systems;*

*(C) does not impose any substantive design, performance, data-handling, documentation, civil liability, taxation, fee, or other requirement on artificial intelligence models, artificial intelligence systems, or automated decision systems unless such requirement—*

*(i) is imposed under Federal law; or*

*(ii) in the case of a requirement imposed under a generally applicable law, is imposed in the same manner on models and systems, other than artificial intelligence models, artificial intelligence systems, and automated decision systems, that provide comparable functions to artificial intelligence models, artificial intelligence systems, or automated decision systems; and*

*(D) does not impose a fee or bond unless—*

*(i) such fee or bond is reasonable and cost-based; and*

*(ii) under such fee or bond, artificial intelligence models, artificial intelligence systems, and automated decision systems are treated in the same manner as other models and systems that perform comparable functions.”*