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

SECTION-BY-SECTION

Sec. 1.
Short Title; table of contents.

Sec. 2.
Defines the following terms and phrases used in the bill: Artificial Intelligence; Artificial General Intelligence; Covered Employee; Quarter; Covered Entity; Frontier AI Model; High-Risk AI System; Sensitive Data; AI-Related Job Effects; Superfund Site.

Sec. 3.
Places a duty of care on AI developers in the design, development, and operation of AI platforms to prevent and mitigate foreseeable harm to users. Additionally, this section requires:

- AI platforms to conduct regular risk assessments of how algorithmic systems, engagement mechanics, and data practices contribute to psychological, physical, financial, and exploitative harms.
- The Federal Trade Commission (FTC) to promulgate rules establishing minimum reasonable safeguards.

Sec. 4.
Requires large frontier developers to draft and implement protocols to manage and mitigate catastrophic risk, publish transparency reports disclosing information about their frontier models, and establish regular reporting to the Department of Homeland Security (DHS). It would:

- Require DHS to establish a mechanism for frontier developers and its employees to anonymously report critical safety incidents.
- Require the Office of Science and Technology Policy (OSTP) to annually assess and make recommendations to update this section.
- Preempt state laws and regulations related to the regulation of frontier AI developers related to the management of catastrophic risk.

Sec. 5.

- Requires certain companies and federal agencies to issue reports on AI-related job effects, including layoffs and job displacement to the Department of Labor (DOL) on a quarterly basis.
- Requires the DOL to compile data on AI-related job effects and publish a report to Congress and the public.

Sec. 6.
Reforms Section 230 by incentivizing the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material. These changes include:

- Establishing a "Bad Samaritan" carve-out that would deny immunity from civil liability to platforms that purposefully facilitate or solicit third-party content that violates federal criminal law.
- Requiring interactive computer services to notify users that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the user limit access to material that is harmful to minors.

Sec. 7.
Requires covered online platforms, including social media platforms, to implement tools and safeguards to protect users and visitors under the age of 17 to protect children from sex trafficking, suicide, and other abuses.

- Covered platforms are online platforms, video games, messaging applications, or video streaming services used or likely to be used by individuals under the age of 17, with limited exceptions.
- This section generally requires covered platforms to exercise reasonable care in the design and use of features that increase minors' online activity to prevent and mitigate harm to minors (e.g., mental health disorders and severe harassment).
- Covered platforms are required to provide certain safeguards to minors, such as protections for minors' data; tools for parents of minors, such as access to minors' privacy settings; and a mechanism for account holders and visitors to report harm to minors on the platform.
- Covered platforms are prohibited from conducting market or product research on children under the age of 13 and may only conduct research on those under the age of 17 with parental consent.
- Enforcement is provided through the FTC and states.
- The section also requires covered platforms to provide users notice when using algorithms and permit users to switch to an algorithm that does not rely on user-specific data.

Sec. 8.
This section establishes requirements for companies providing AI chatbot and companion services to protect kids.

Sec. 9.

- Establishes an "Advanced Artificial Intelligence Evaluation Program" within the Department of Energy (DOE) to evaluate advanced AI systems and collect data on the likelihood of adverse AI incidents, such as loss-of-control scenarios and weaponization by adversaries.
- Requires developers of advanced AI systems to participate in the program, including a duty to provide information regarding the AI system upon request.
- Prohibits an advanced AI system from being deployed until the developer has complied with program requirements.

Sec. 10.
Enables the U.S. Attorney General, state attorneys general, and private actors to file suit to hold AI system developers liable for harms caused by the AI system for defective design, failure to warn, express warranty, and unreasonably dangerous or defective product claims. If an AI system deployer substantially modifies an AI system or intentionally misuses an AI system contrary to its intended use, the deployer could also be held liable.

Sec. 11.
Combats the consistent pattern of bias against conservative figures demonstrated by Big Tech and AI systems by requiring:

- Audits of high-risk AI systems to undergo regular bias evaluations to prevent discrimination based on protected characteristics, including political affiliation.
    - High-risk AI systems cover those that could pose significant risks to health, safety, rights, or economic security, including those in education, employment, law enforcement, or critical infrastructure.
- Federal agencies and covered entities to provide AI ethics training to personnel.
    - Covered entities are any person, partnership, corporation, or other entity engaged in the development, deployment, or operation of AI systems, including federal agencies, that meet thresholds established by the FTC.

Sec. 12.
Establishes the Federal AI Safety Institute (FAISI) within the National Institute of Standards and Technology (NIST).

- FAISI would:
    - Conduct unclassified evaluations of AI risks, including cybersecurity and biosecurity.
    - Develop voluntary agreements with private sector developers.
    - Standardize safety testing protocols for frontier models.
    - Coordinate with international partners.
    - Submit annual recommendations to Congress on AI oversight.

Sec. 13.
This section establishes the National Artificial Intelligence Research Resource (NAIRR) to remove barriers to essential tools and infrastructure that power artificial intelligence research and development. Specifically, this section would:

- Make computing resources, massive datasets, and advanced infrastructure required to perform cutting-edge research in AI available to students, researchers, non-profits, small businesses, and academic institutions as a shared resource.
- Establish a formal governance structure for NAIRR, including a Steering Subcommittee under OSTP and a Program Management Office within the NSF to oversee operations, manage federal and private resource contributions, select an independent operating entity through a transparent bidding process, and ensure adherence to strict standards of privacy, ethics, scientific integrity, and national security.
- Require NAIRR be built using donated resources from both federal agencies and the private sector.

Sec. 14.

- Covered entities pursuing artificial general intelligence development shall submit annual progress reports to the Federal AI Safety Institute.

Sec. 15.
Requires:

- The Office of Management and Budget (OMB) and the General Services Administration (GSA) to establish an interagency process, in coordination with the Environmental Protection Agency

(EPA), the Department of the Interior (DOI), and other relevant agencies, for the designation of remediated superfund sites and federal lands as suitable for housing, data centers, or electricity generation and storage.
- In making designations, the interagency process to prioritize sites that minimize environmental impact, support AI infrastructure needs, and promote economic development.
- The GSA to publish initial decisions within 180 days of the effective date of this Act and update them annually.

Sec. 16.
Establishes a "Veterans and Workforce Housing Fund" to be administered by the Department of Housing and Urban Development (HUD) for the construction of veteran housing and middle-class workers.

Sec. 17.
Requires data center operators to be responsible for the full cost of all energy and water infrastructure needed for their operation, including construction, maintenance, and upgrades with no impact on ratepayers.

Sec. 18.
- Creates a federal right for individuals to sue companies for using their data (personal, copyrighted) for AI training without explicit consent.
    - "Covered data" includes personally identifiable information, biometrics, geolocation, browsing history, and copyrighted works.
- Requires affirmative consent for data use in AI models, addressing issues like unauthorized scraping of creative works.
- Allows for statutory damages, punitive damages, injunctions, and attorney fees.
- Invalidates clauses forcing pre-dispute arbitration or class-action waivers for these claims.

Sec. 19.
This section addresses the use of non-consensual digital replications in audiovisual works, images, or sound recordings. Specifically, this section would:
- Hold individuals or companies liable if they produce an unauthorized digital replica of an individual in a performance.
- Hold platforms liable for hosting an unauthorized digital replica if the platform has actual knowledge of the fact that the replica was not authorized by the individual depicted.
- Exclude certain digital replicas from coverage based on recognized First Amendment protections.
- Largely preempt state laws addressing digital replicas to create a workable national standard.

Sec. 20.
Deems derivative works generated, synthesized, or produced by an AI system without authorization as infringing works, which would be ineligible for copyright protection.
- The absence of human authorship, or the use of automated computational processes, would not limit a finding of infringement under this subsection.
- AI developers, operators, and distributors would be required to publish a Training Data Use Record and an Inference Data Use Record. For inferences models that continuously access new content, monthly updates would be required.

- The FTC would enforce this section with significant statutory fines.

Sec. 21.

- Establishes a limited, conditional safe harbor permitting copyright owners to collectively license works for specified AI uses without per se antitrust liability.
- Creates registration, oversight, and enforcement mechanisms to ensure collective licensing organizations operate transparently and competitively.
- Preserves and promotes competition among AI developers by mandating nondiscriminatory access to licensed content.
- Protects copyright owners' rights to license individually, withdraw from collective arrangements, and receive fair compensation.
- Establishes efficient arbitration procedures for rate determination to ensure reasonable compensation while maintaining AI development viability.
- Prevents extension of collective licensing authority into downstream product markets, advertising, or content distribution.

Sec. 22.

This section requires companies to give American businesses first priority in acquiring advanced AI chips before exporting these chips to China and other countries of concern.

Sec. 23.

- Requires interoperability for systemically important platforms, which include platforms with subscribers or monthly active users in the United States not less than 34% of the population of the United States.
- Prevents systemically important platforms from using data generated on the platform to compete with products or services offered by business users on the platform.
- Prevents systemically important platforms from self-preferencing or steering users to products or services offered by the platform operator. It would also prevent data from being transferred to the PRC or other foreign adversaries.
- Prevents systemically important platforms from disseminating sexual material harmful to minors.
- If a civil action is brought against a systemically important platform under this section or any antitrust law, the matter shall be assigned for expeditated priority consideration, which results in a decision within one year.

Sec. 24.

The Act does not preempt any generally applicable law, including a body of common law or a scheme of sectoral governance that may address artificial intelligence.

Sec. 25.

If any provisions are found to be invalid, the remaining provisions may still be enforced.

Sec. 26.

The Act becomes effective 180 days after enactment.