From Principles to Policy: Enabling 21st Century AI Innovation in Financial Services

Testimony of J.B. Branch, Big Tech Accountability Advocate, Public Citizen, before the House Committee on Financial Services

@jbbranch.bsky.social

December 10, 2025

PUBLICCITIZEN

December 10, 2025

Chairman French Hill and Ranking Member Maxine Waters
U.S. House Committee on Financial Services
U.S. House of Representatives
2128 Rayburn House Office Building
Washington, D.C. 20515

Chairman Hill, Ranking Member Waters, and Members of the Committee:

I am J.B. Branch, the Big Tech Accountability Advocate at Public Citizen and an expert in Artificial Intelligence (AI) governance. Public Citizen is a national nonprofit consumer advocacy organization with more than one million members and supporters nationwide. Since our founding in 1971, we have worked to ensure that government and corporate power are transparent, accountable, and responsive to the public interest. Public Citizen was at the forefront of responsible AI long before ChatGPT became mainstream. Our research and policy analysis has consistently warned of the very harms we witness today including AI-related threats to democracy, consumer manipulation and harm, worsening inequality, abusive working conditions, AI usage in warfare, and environmental impacts related to AI.[1]

In the context of emerging technologies, Public Citizen advocates for innovation that is tethered to enforceable safeguards, democratic oversight, and meaningful public accountability. We commend the Committee for convening this hearing to examine the future of AI policy at a moment of extraordinary technological acceleration and public risk.

There is no doubt that AI will shape the American economy, workforce, national security, and democratic institutions for generations to come. **The only real question before Congress is who this technology will ultimately serve: the public or a narrow set of powerful corporate actors insulated from public accountability.** As this Committee

[1] Rick Claypool and Cheyenne Hunt, *Sorry in Advance!*, Public Citizen, April 18, 2023, https://www.citizen.org/article/sorry-in-advance-generative-ai-artificial-intellligence-chatgpt-report/; Craig Holman, *The Nature and Risks of AI-Generated Deepfakes in Political Communications*, Public Citizen, October 10, 2025,https://www.citizen.org/article/the-nature-and-risks-of-ai-generated-deepfakes-in-political-communications/; Robert Weissman and Savannah Wooten, *A.I. Joe: The Dangers of Artificial Intelligence and the Military*, Public Citizen, February 29, 2024, https://www.citizen.org/article/ai-joe-report/; Deanna Noel and Meghan Pazik, *Reigning in Big Tech: Policy Solutions to Address the Data Center Buildout*, Public Citizen, December 3, 2025, https://www.citizen.org/article/reining-in-big-tech-policy-solutions-to-address-the-data-center-buildout/; Tyson Slocum, *Congressional Testimony on Artificial Intelligence Data Centers Energy Needs*, Public Citizen, April 1, 2025, https://www.citizen.org/article/congressional-testimony-artificial-intelligence-data-center-energy/

considers questions of U.S. leadership in AI, Public Citizen urges lawmakers to recognize that AI will not be determined by stock prices or server capacity, but by whether our democratic institutions can still govern powerful technologies in the public interest. **Leadership within innovation requires moral clarity, civil rights protections, worker safeguards, consumer safety, and democratic governance.**

Public Citizen's work has shown that the harms associated with AI are no longer speculative. From deepfake election interference[2] and AI-generated child sexual abuse material[3] to automated discrimination,[4] workplace surveillance,[5] and large-scale fraud,[6] AI systems are already producing real-world damage at scale. National intelligences agencies,[7] consumer protection regulators,[8] and child safety organizations[9] have repeatedly warned that AI has become a force multiplier for deception, criminal exploitation, and consumer harm.

At the same time, Congress is being pressed to pursue sweeping deregulatory proposals under the banner of "innovation." This includes efforts to preempt state AI laws, weaken regulatory agencies, and the grant of broad immunity to AI developers. **Public Citizen strongly rejects the false premise that regulation and competitiveness are mutually exclusive.** The lesson of every major technological revolution, from railroads to pharmaceuticals to social media, is that the absence of early guardrails does not accelerate progress—it multiplies harms, destabilizes markets, and erodes public trust.

This testimony addresses six core issues now directly before this Committee: (1) persistent efforts to undermine state AI protections; (2) the politicization of fairness in AI

---

[2] Claudia Koon Ghee Wee, *Artificial Illusion: Global Governance Challenges of Deepfake Technology*, IAPP, April 23, 2025, https://iapp.org/news/a/artificial-illusion-global-governance-challenges-of-deepfake-technology

[3] Rianna Pfefferkorn, *Addressing AI-Generated Child Sexual Abuse Material: Opportunities for Educational Policy*, Stanford Human-Centered Artificial Intelligence, July 21, 2025, https://hai.stanford.edu/policy/addressing-ai-generated-child-sexual-abuse-material-opportunities-for-educational-policy

[4] Quinn, Emanuel, Urquhart, and Sullivan LLP, *When Machines Discriminate: The Rise of AI Bias Lawsuits*, Quinn Emanuel, August 18, 2025, https://www.quinnemanuel.com/the-firm/publications/when-machines-discriminate-the-rise-of-ai-bias-lawsuits/

[5] AFL-CIO, *Artificial Intelligence: Principles to Protect Workers*, October 15, 2025, https://aflcio.org/reports/workers-first-ai

[6] FBI, *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*, Alert Number: I-120324-PSA, December 3, 2025, https://www.ic3.gov/PSA/2024/PSA241203

[7] FBI, *FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence*, May 8, 2024, https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

[8] Darren M. Walsh and Stuart D. Levi, *CFPB Comments on AI Offer Insights for Consumer Finance Industry*, August 23, 2024, https://www.skadden.com/insights/publications/2024/08/cfpb-comments-on-artificial-intelligence

[9] Associated Press, *Advocacy Groups Urger Parents to Avoid AI Toys this Holiday Season*, November 21, 2025, https://www.kcra.com/article/ai-toys-safety-holiday-warning/69512613

governance; (3) the risks of politically driven censorship within AI; (4) the exploitation of workers and communities throughout the AI stack; (5) the growing risks posed by AI in the financial sector; and (6) the mounting evidence that the tech industry may be entering an AI investment bubble.

Public Citizen submits this testimony to urge Congress to abandon the deregulatory shortcuts of the past and instead build a durable federal AI framework that protects families, workers, consumers, civil rights, democratic institutions, and economic stability. That framework must establish a strong federal floor of protection while preserving the authority of states to respond to emerging harm in real time, especially as AI evolves faster than the currently polarized and paralyzed congressional process can realistically move. The stakes are no longer hypothetical. The harms are multiplying. The financial exposure continues to balloon. And the public remains vulnerable due to Congressional inaction.

I. Persistent Efforts to Undermine State AI Protections

In the absence of comprehensive federal AI legislation, states have emerged as the primary arena of meaningful AI governance in the United States. Over the past several years, state legislatures across the country have enacted bipartisan protections addressing deepfake abuse, algorithmic discrimination, biometric surveillance, automated hiring, consumer deception, and child safety. These laws reflect democratic will in action. They are not theoretical policy exercises. They are pragmatic responses to real-world harms that communities are already experiencing and demanding accountability.

Yet rather than build upon this state-led momentum, powerful interests in Washington pursue a coordinated campaign to dismantle it. Earlier this year, Republicans advanced one of the most sweeping deregulatory proposals in the history of U.S. technology policy: a federal AI moratorium that would have frozen the enforcement of state AI laws nationwide.[10] The proposal would have barred states from enforcing existing protections for years at precisely the moment when AI-generated fraud, deepfake abuse, consumer deception, and automated discrimination are accelerating.[11]

This proposal was extraordinary not only for its breadth, but for what it represented philosophically: a declaration that democratic state action must be suspended to preserve corporate freedom from oversight. The American public rejected that premise decisively.

---

[10] Anthony Adragna, '*Not at all Dead': Cruz says AI Moratorium will Return*, Politico, September 16, 2025, https://www.politico.com/news/2025/09/16/not-at-all-dead-cruz-says-ai-moratorium-will-return-00566369

[11] *Id*.

Ninety-seven percent of Americans agree that AI safety and security should be subject to rules and regulations, according to a Gallup poll.[12] In a rare moment of near-unanimity, the U.S. Senate defeated the moratorium proposal by a 99–1 vote,[13] delivering a bipartisan rebuke to the idea that AI companies should be shielded from accountability through federal fiat.

That vote should have ended the debate. It did not. After the moratorium failed, proponents attempted a quieter route. Behind the scenes, and at the final hour, Republicans tried to sneak in nearly identical AI preemption language into the National Defense Authorization Act (NDAA)—a must-pass national security bill traditionally reserved for military funding, not sweeping technology deregulation.[14]

This maneuver was deeply troubling for three reasons. First, it attempted to use the urgency of national defense as political cover for sweeping corporate immunity in hopes that the American public and civic tech advocates were not being vigilant. Second, it sought to override state civil rights, consumer protection, and child safety laws without public debate, hearings, or meaningful scrutiny. Thirdly, it continued Republican efforts to pursue blanket corporate immunity in an entirely unrelated must-pass legislative vehicle. This was not governance. It was a deliberate attempt to subordinate the democratic process to corporate privilege.

Once again, bipartisan opposition prevailed.[15] The preemptive language was ultimately kept out. But the strategy was unmistakable: when transparency fails, try stealth.

Most recently, obsession over this poorly considered deregulatory campaign has moved into President Trump's executive branch. A leaked draft executive order would reportedly direct the Department of Justice to actively challenge state AI laws on the grounds that they "burden interstate commerce" and interfere with federal priorities.[16] In effect, this order would weaponize federal litigation to achieve what Congress refused to authorize: nationwide invalidation of state AI protections.[17]

---

[12] Benedict Vigers and Justin Lall, *Americans Prioritize AI Safety and Data Security*, Gallup News, September 16, 2025, https://news.gallup.com/poll/694685/americans-prioritize-safety-data-security.aspx
[13] U.S. Senate, *Senate Strikes AI Moratorium from Budget Reconciliation Bill in Overwhelming 99-1 Vote*, July 1, 2025, https://www.commerce.senate.gov/2025/7/senate-strikes-ai-moratorium-from-budget-reconciliation-bill-in-overwhelming-99-1-vote/8415a728-fd1d-4269-98ac-101d1d0c71e0
[14] Julia Shapero and Sudiksha Kochi, *AI Showdown Splits Republicans in High-Stakes NDAA Talks*, The Hill, December 2, 2025, https://thehill.com/policy/technology/5628534-trump-lawmakers-battle-ai/
[15] Ashley Belanger, *Republicans Drop Trump-ordered Block on State AI Laws from Defense Bill*, ArsTechnica, December 3, 2025, https://arstechnica.com/tech-policy/2025/12/republicans-once-again-thwart-trumps-push-to-block-state-ai-laws/
[16] Public Citizen, *Legal Analysis of Leaked Draft AI Preemption Executive Order*, November 21, 2025, https://www.citizen.org/article/legal-analysis-of-leaked-draft-ai-preemption-executive-order/
[17] *Id*.

If finalized, such an order would represent an unprecedented, reckless and illegal misuse of executive power to extinguish state consumer protection, civil rights, and child safety laws in service of industry demands. It would bypass Congress, override state legislatures, and concentrate extraordinary regulatory power inside the White House. This is precisely the opposite of democratic governance.

Taken together, these three efforts—the failed federal moratorium, the NDAA insertion attempt, and the leaked executive order—are not isolated events. They form an intentional Republican strategy backed by Big Tech political spending: (1) Freeze state enforcement through Congress; (2) if that fails, smuggle preemption into must-pass legislation; (3) and finally, override states through executive action. Each step moves further away from democratic accountability and closer to centralized corporate immunity.

All of this is at the behest of the AI industry, which argues that their companies should not be governed by the same rule of law that applies to every other powerful industry in America. Big Tech companies, who have invested heavily in AI, have also invested heavily in political spending. Between 2024 and 2025 large tech or electronic companies have spent over $764.5 million in political spending.[18] Over 75 percent of this was donated to Republican candidates and nearly half (46 percent) came from Elon Musk alone.[19]

It is important to underscore that states did not rush to regulate AI because of political ideology. They acted because Congress has failed to enact meaningful AI regulations. States legislated because deepfake exploitation,[20] automated discrimination,[21] biometric surveillance,[22] and AI-driven scams were already harming their residents.[23] To now strip those protections miles away in Washington, D.C.—after communities have debated them, passed them on a bipartisan basis, and begun enforcing them—would be a direct assault on federalism, democratic self-governance, and public trust.

This strategy leverages preemption, not as a floor for protection, but as a ceiling for accountability. Moreover, Congressional Republicans have not provided any meaningful

---

[18] Rick Claypool, *Robo-Trump: Big Tech's Big Spending and the Republican Effort to Delete State Laws Against AI Harms*, Public Citizen, November 21, 2025, https://www.citizen.org/article/robo-trump-big-tech-big-spending-and-republican-effort-delete-state-ai-laws/

[19] *Id*.

[20] Ilana Beller, *Tracker: State Legislation on Deepfakes in Elections*, Public Citizen, October 20, 2025, https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/

[21] Gabrielle Martin, *Illinois Enacts New AI Legislation, Joining Colorado as the Only States Regulating Algorithmic Discrimination in Private Sector use of AI Systems (US)*, Employment Law Worldview, August 19, 2024, https://www.employmentlawworldview.com/illinois-enacts-new-ai-legislation-joining-colorado-as-the-only-states-regulating-algorithmic-discrimination-in-private-sector-use-of-ai-systems-us/

[22] Bobby Allyn, *With no Federal Facial Recognition Law, States Rush to Fill Void*, NPR, August 28, 2025, https://www.npr.org/2025/08/28/nx-s1-5519756/biometrics-facial-recognition-laws-privacy

[23] Bryan Cave Leighton Paisner, *US State-by-State AI Legislation Snapshot*, https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html

AI governance alternative. Instead, they seek to replace real-world safeguards with a vacuum. Those who are supporting federal preemption seem to believe in voluntary corporate promises. The past two decades of technologically driven social media harm should serve as a lesson that promises from the tech industry should not be taken at face value.

The public has learned from Congressional leaders' failure to reign in Big Tech companies during the social media experimentation of the early 2000s. While tech companies argued that Section 230 was an absolute necessity or that Congress should lean on their expertise, they unleashed onto the world a variety of harms that we have yet to control. Those harms include harmful algorithmic steering to children including self-harm and eating disorders;[24] election misinformation that challenges global stability;[25] and a toxic online atmosphere that has created echo chambers online while destroying neighborhoods in the real world.[26]

Congress must learn from past mistakes and stand vigilant of AI just as the American public has. Polling demonstrates Americans reject the tech industries push to self-regulate AI by a 6-1 margin.[27] This includes 72% of Americans who prefer slowing down the development of AI and 82% of voters who say they don't trust tech company executives to self-regulate.[28] The American people are not asking for a pause on accountability. They are asking for protection. And the states have already begun to deliver.

II. The Politicization of Fairness and Civil Rights in AI Governance

As efforts to dismantle state AI protections have accelerated, a parallel and equally dangerous trend has emerged: the deliberate politicization of fairness, nondiscrimination, and civil rights in artificial intelligence governance. In recent years, some policymakers have sought to rebrand our most basic Constitutional principles as "ideological," "woke," or even "dangerous." This reframing is not accidental. It is a strategic effort to delegitimize civil rights enforcement throughout the U.S.

---

[24] Center for Countering Digital Hate, *YouTube's Anorexia Algorithm: How YouTube Recommends Eating Disorder Videos to Young Girls*, December 10, 2024, https://counterhate.com/research/youtube-anorexia-algorithm/

[25] Danielle Draper and Sbine Neschke, *The Pros and Cons of Social Media Algorithms*, October 2023, Bipartisan Policy Center, https://bipartisanpolicy.org/wp-content/uploads/2023/10/BPC_Tech-Algorithm-Tradeoffs_R01.pdf

[26] Jennifer Ouellette, *Study: Social Media Probably can't be Fixed*, ArsTechnica, August 13, 2025, https://arstechnica.com/science/2025/08/study-social-media-probably-cant-be-fixed/

[27] Sarah Fortinsky, *Majority of Americans are Concerned about Rapidly Developing AI: Poll*, The Hill, August 9, 2023, https://thehill.com/homenews/4145203-majority-of-americans-are-concerned-about-rapidly-developing-ai-poll/

[28] *Id*.

But at its core, algorithmic fairness simply means that automated systems should not produce discriminatory outcomes based on race, gender, religion, disability, age, or other protected characteristics.[29] That principle is neither novel nor partisan. It is embedded in decades of U.S. civil rights law, including the Civil Rights Act of 1964,[30] the Fair Housing Act,[31] the Equal Credit Opportunity Act,[32] and the Voting Rights Act.[33]

Yet today, those same nondiscrimination principles are increasingly being recast as political ideology when applied to AI. The Trump administration's own "Woke AI" executive order claims efforts to prevent biased algorithmic outcomes amount to "ideological biases or social agendas."[34] This perversion of reality turns the Constitution on its head.

Equal protection under the law is not an ideology. It is quite literally the law and a principle underlying the premise of the American Dream. When policymakers treat civil rights as optional or partisan in the AI context, they are not defending neutrality. They are authorizing discrimination by default.

From a technical and legal perspective, fairness in AI governance involves three basic obligations:

1. **Bias detection and mitigation:** Developers must test for disparate impacts before deployment.[35]
2. **Transparency and auditability:** Regulators and impacted users must be able to examine how decisions are made.[36]
3. **Legal accountability:** When automated systems violate civil rights, there must be clear avenues for enforcement and remedy.[37]

---

[29] Stanford Encyclopedia of Philosophy, *Algorithmic Fairness*, July 30, 2025, https://plato.stanford.edu/entries/algorithmic-fairness/
[30] Civil Rights Act of 1964, 42 U.S.C. § 2000, Pub. L. No. 88-352, 78 Stat. 241 (1964).
[31] Fair Housing Act, 42 U.S.C. § 3601–3619 (1968 & Supp. V 2023) (amended by Pub. L. 90–284).
[32] Equal Credit Opportunity Act, 15 U.S.C. § 1691 (2020).
[33] Voting Rights Act of 1965, Pub. L. 89-110, 79 Stat. 437.
[34] President Donald J. Trump, *Preventing Woke AI in the Federal Government*, Exec. Order No. 14099 (July 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government
[35] Kate Goddard, Abdul Roudsari & Jeremy C. Wyatt, *Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators*, 19 J. Am. Med. Inform. Assoc. 121 (Jan.–Feb. 2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3240751/
[36] Nagadivya Balasubramaniam et al., *Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements*, 159 Info. & Software Tech. 107197 (2023), https://www.sciencedirect.com/science/article/pii/S0950584923000514.
[37] NTIA, *Liability Rules and Standards*, in *AI Accountability Policy Report: Using Accountability Inputs*, Mar. 27, 2024, https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/using-accountability-inputs/liability-rules-and-standards

These principles already govern credit decisions,[38] employment screening,[39] housing access,[40] and voting protections.[41] AI does not change the need for civil rights enforcement; it amplifies it. Automated systems can now deny loans,[42] screen out job applicants,[43] flag people for surveillance,[44] and influence elections on a scale never seen before, often without human oversight.[45]

When lawmakers suggest that addressing these harms is suspect, the result is not neutral. The result is that companies deploying high-risk systems profit while impacted communities are left with no meaningful recourse. **Public Citizen's position is straightforward: civil rights are a legal and moral obligation.** Congress cannot meaningfully claim leadership in responsible AI while allowing the foundational principle of equal protection to be caricatured as partisan ideology.

[38] *See supra* note 32.
[39] 42 U.S.C. § 2000e-2(a)(1) (prohibits discrimination in employment).
[40] *See supra* note 31.
[41] *See supra* note 25.
[42] Lehigh University News, *AI Exhibits Racial Bias in Mortgage Underwriting Decisions*, Lehigh University News (Aug. 20, 2024) https://news.lehigh.edu/ai-exhibits-racial-bias-in-mortgage-underwriting-decisions
[43] Stefane Milne, *AI tools show biases in ranking job applicants' names according to perceived race and gender*, UW News (Oct. 31, 2024) https://www.washington.edu/news/2024/10/31/ai-bias-resume-screening-race-gender/
[44] Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy Is an Imperative for Communities of Color*, Brookings (Apr. 12, 2022) https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/
[45] Amy Hamblin, *Tackling the Threat of Deepfakes in Our Elections*, NextGen Policy (Oct. 17, 2024), https://www.nextgenpolicy.org/lets-talk/tackling-the-threat-of-deepfakes-in-our-elections/.

III. Federal Inconsistency and the Risks of Politically Driven AI Deployment

Even as some policymakers seek to dismantle state protections and recast civil rights as "ideological," the federal government's own conduct with respect to AI reveals a troubling pattern of internal inconsistency and politically driven deployment. On paper, federal AI policy emphasizes safety, transparency, and public trust.[46] In practice, those commitments are increasingly undermined by contradictory actions that prioritize speed, political loyalty, and corporate alignment over public protection. This inconsistency directly weakens the credibility of federal AI governance and signals to industry that safety principles are negotiable.

These commitments mirror global norms reflected in international frameworks and emerging foreign AI laws.[47] They also align with long-standing U.S. traditions of consumer protection, civil rights enforcement, and product safety regulation. Yet at the same time, high-risk AI systems continue to be fast-tracked into sensitive federal contexts without the level of independent testing, auditability, or public disclosure that these very principles require. When safety frameworks exist primarily on paper, they become aspirational rather than enforceable. Put simply, aspirational governance is not governance at all.

The federal government's procurement of Elon Musk's Grok system is a stark example of this breakdown between stated principle and actual practice.[48] Grok has been publicly documented engaging in racist and antisemitic tirades,[49] spreading conspiratorial content,[50] and even referring to itself as "Mecha Hitler."[51] These are not edge cases or obscure technical glitches. They are clear signals that the system does not meet even basic standards of safety, non-discrimination, or reliability that federal AI policy claims to uphold.

---

[46] Office of Management and Budget, Executive Office of the President, *Memorandum for the Heads of Executive Departments and Agencies, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust,* M-25-21, (April 3, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf ("OMB M-25-21");
Office of Management and Budget, Executive Office of the President, *Memorandum for the Heads of Executive Departments and Agencies, Driving Efficient Acquisition of Artificial Intelligence in Government,* M-25-22, (April 3, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf ("OMB M-25-22").
[47] IAPP, *Global AI Law and Policy Tracker*, https://iapp.org/resources/article/global-ai-legislation-tracker/
[48] U.S. General Services Administration, *GSA and xAI Partner on $0.42 per Agency Agreement to Accelerate Feederal AI Adoption*, September 25, 2025, https://www.gsa.gov/about-us/newsroom/news-releases/gsa-xai-partner-to-accelerate-federal-ai-adoption-09252025
[49] Lisa Hagen, Huo Jingnan & Audrey Nguyen, *Grok AI Produces Antisemitic, Racist Content on X*, NPR (July 9, 2025), https://www.npr.org/2025/07/09/nx-s1-5462609/grok-elon-musk-antisemitic-racist-content.
[50]Derek Robertson, *Grok's 'White Genocide' Glitch and the AI Black Box*, Politico (May 15, 2025), https://www.politico.com/newsletters/digital-future-daily/2025/05/15/groks-white-genocide-glitch-and-the-ai-black-box-00352709
[51] Dylon Jones, *How Musk's Grok Chatbot Ended up Praising Hitler*, Politico Magazine (July 10, 2025), https://www.politico.com/news/magazine/2025/07/10/musk-grok-hitler-ai-00447055.

Moving a system with this record toward federal deployment is not a neutral technical choice. It is a policy decision to tolerate behavior that would be unacceptable from any human federal employee[52] unless, apparently, they happened to be President Trump's donor or friend.[53] It directly contradicts commitments to protect civil rights, prevent harmful content, and ensure trustworthy AI in government operations. It tells the market that adherence to federal AI principles is optional when politically connected vendors are involved.

That signal carries real consequences, because the federal government is one of the largest contract purchasers in the world.[54] That purchasing power shapes markets, sets standards, and confers legitimacy. When AI systems are deployed across federal agencies, they are not merely tools. They become symbols of official approval by the U.S. government, and by proxy, the American people.

Politicized procurement, where alignment with political leadership or ideological agendas substitutes for independent technical and civil rights evaluation, creates several systemic risks:

1. **Erosion of public trust:** Citizens are less likely to trust automated systems that appear to reflect political priorities rather than neutral safety standards.
2. **Regulatory capture through the back door:** Procurement becomes a substitute for regulation, granting practical immunity to selected vendors.
3. **Institutional lock-in:** Once embedded in federal infrastructure, flawed AI systems become costly and difficult to unwind.
4. **Export of unsafe norms:** U.S. procurement decisions influence what other governments adopt as acceptable practice.

In short, federal deployment choices now function as *de facto* global standard-setting. That power carries responsibility. But it is not being exercised with sufficient restraint.

The United States does not regulate AI in a vacuum. Federal policy choices send powerful signals to allies, adversaries, and multinational corporations. When U.S. institutions appear to downplay safety, weaken civil rights protections, or politicize algorithmic governance, those signals travel globally.

At a time when democratic governments are struggling to articulate credible alternatives to digital authoritarianism, inconsistency in U.S. AI governance weakens the moral

---

[52] U.S. Department of Labor, *OSHA Workers Rights and Protections*, https://www.osha.gov/workers
[53] Rachel Leingang, *Trump Nominee Reportedly Boasted of 'Nazi Streak' in Group Chats*, The Guardian, October 20, 2025, https://www.theguardian.com/us-news/2025/oct/20/trump-nominee-paul-ingrassia-group-chats
[54] K & L Gates Public Policy and Law Practice, *Government Contracts and Procurement*, K&L Gates 2011, https://files.klgates.com/files/upload/public_policy_govt_contracts.pdf

authority of democratic oversight worldwide. A government that cannot consistently apply its own principles at home is poorly positioned to advocate for rights-respecting AI abroad.

Public Citizen urges Congress to recognize that federal inconsistency is not a neutral condition. It actively destabilizes trust, weakens civil rights enforcement, and invites corporate opportunism. If AI is to serve the public, the rules governing its deployment must be stable, enforceable, and insulated from political expediency.

IV. The Exploitation of Workers and Communities Through AI Infrastructure and Automation

As AI reshapes the economy, its physical and economic footprint is increasingly borne by workers and communities that are promised prosperity but too often receive disruption, higher costs, and fewer protections. Nowhere is this more evident than in the rapid buildout of data center infrastructure and the accelerating deployment of workplace automation.

Across the country, particularly in rural and economically distressed regions, communities are told that data centers and AI infrastructure represent the next great engine of economic revitalization.[55] State and local governments are encouraged to offer generous tax abatements, discounted electricity rates, land concessions, and expedited permitting in exchange for the promise of "high-tech jobs" and long-term economic growth.[56]

This narrative is powerful. It is also misleading.

Data centers sit at the very bottom of the technology value chain. Their construction phase may generate a brief surge in temporary jobs, but once operational, most facilities require only a small permanent workforce. The largest data centers employ roughly 100 to 200 employees.[57] This is less employees than hired at a Walmart Superstore.[58] Meanwhile, the long-term economic burdens remain local: higher electricity prices, strained grids, increased water usage, and land converted to infrastructure that produces little sustained community wealth.[59]

---

[55] *See supra* note 1, Tyson Slocum testimony.
[56] *Id*.
[57] Tom Dotan, *The AI Data-Center Boom is a Job-Creation Bust*, February 25, 2025, The Wall Street Journal, https://www.wsj.com/tech/ai-data-center-job-creation-48038b67?gaa_at=eafs&gaa_n=AWEtsqeTcyMiO56lqVqVS2H8r9XX6qes4JPflj8qfDi38-ItKJdVIkx4V7rhXIogfJI%3D&gaa_ts=6935ae60&gaa_sig=x0Rel4IeIrITOxtbZTHIZzYFWB4lRcklNQd7yT0tuosyop1qgcOtgF24d8G9-YfhKICzdtFqYVGVfA7tPWg1Kw%3D%3D
[58] Matthew Yglesias, *Maybe Wal-Mart Should Hire Some People*, Slate, April 4, 2025, https://slate.com/business/2013/04/wal-mart-labor-saving-gone-too-far-superstore-needs-to-hire-some-people.html
[59] *See supra* note 1, Tyson Slocum testimony.

Americans have seen this story before. Steel towns were promised stability. Shale gas communities promised prosperity. Offshoring was supposed to create "new opportunities." Each cycle left workers more exposed, and communities more fragile. AI infrastructure is now being sold with the same familiar optimism and the same thin guarantees.

AI data centers are also among the most energy-intensive industrial facilities ever deployed.[60] Their electricity demand is measured in orders of magnitude. In many regions, utilities are already signaling that residential and small business ratepayers will bear the cost of grid expansion required to serve hyperscale AI infrastructure.[61]

This creates a deeply inequitable cost shift. Working families, many of whom will never directly benefit from AI development, are being asked to subsidize some of the wealthiest corporations on the planet. Meanwhile, environmental review processes are frequently accelerated or weakened in the name of "innovation competitiveness."[62] If AI is truly a national priority, then its infrastructure costs should be borne transparently and fairly—not quietly shifted onto households least able to absorb them.

Beyond physical infrastructure, AI is transforming the workplace itself. Employers are rapidly adopting AI systems for:

- **Productivity monitoring and worker surveillance**[63]
- **Automated scheduling and performance scoring**[64]
- **Hiring, promotion, and termination decisions**[65]
- **Task automation and workforce "optimization"**[66]

These systems are often introduced without collective bargaining, meaningful transparency, or worker consent.[67] Employees are essentially asked to trust algorithms they cannot inspect, challenge, or meaningfully appeal. The result is a profound shift in workplace power. Decisions are being moved away from human judgment and toward opaque automated control.

Without guardrails, AI-driven management systems can suppress wages, accelerate burnout, intensify monitoring, and undermine organizing rights.[68] And when displacement occurs, workers are often offered vague assurances of "reskilling" that do not match the scale or speed of job loss.

---

[60] *Id*.
[61] *Id*.
[62] *Id*.
[63] *See supra* note 5.
[64] *Id*.
[65] *Id*.
[66] *Id*.
[67] *Id*.
[68] *Id*.

"Reskilling" initiatives are often highlighted as a solution to workplace automation.[69] While retraining is important, history counsels caution. Often automation produces far fewer high-quality replacement jobs than were promised and, if created, those jobs are less visible and difficult to find.[70] Further, AI-driven displacement is unfolding at a speed that makes traditional retraining pipelines inadequate by comparison.[71] Many of the jobs being automated are entry-level and mid-skill positions that historically served as rungs on the economic ladder.[72] When those rungs disappear, the ladder itself ceases to exist.

A workforce policy built on aspirational retraining slogans is not a workforce policy at all. It is an abdication of responsibility that fits squarely within a broader political tradition of weakening labor protections and undermining unions in the name of "flexibility" and corporate efficiency.

If AI is to strengthen the middle class rather than hollow it out, Congress must intervene now—before infrastructure lock-in and automated management systems become permanent features of the economic landscape. The AI industry's strategy follows the same political logic that has weakened labor standards and targeted unions for decades: move fast for corporations, move slow for workers. Now it's been rebranded as 'AI transition policy'—same script, same winners, same losers. **Public Citizen's believes AI must not become another chapter in the long American history of privatized gains and socialized losses**.

---

[69] Jorge Tamayo et. al., *Reskilling in the Age of AI*, Harvard Business Review, September—October 2023, https://hbr.org/2023/09/reskilling-in-the-age-of-ai?utm_medium=paidsearch&utm_source=google&utm_campaign=domcontent&utm_term=Non-Brand&tpcc=paidsearch.google.dsacontent&gad_source=1&gad_campaignid=20553599500&gbraid=0AAAAAD9b3uRf6T8iE3uqi0-sm_UAx65Uk&gclid=Cj0KCQiA6NTJBhDEARIsAB7QHD1sVmbOBnqOoPgcZZcJJDzBmygO4-VBioWB2UCGkLrjHOKspbK2K_IaAsv2EALw_wcB

[70] James Manyika et. al., *Jobs Lost, Jobs Gained: What the Future of Work will Mean for Jobs, Skills, and Wages*, McKinsey & Company, November 28, 2017, https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

[71] Samantha Subin, *AI is Already Taking White-Collar Jobs. Economists Warn there's 'much more in the tank'*, CNBC, October 22, 2025, https://www.cnbc.com/2025/10/22/ai-taking-white-collar-jobs-economists-warn-much-more-in-the-tank.html

[72] Till Leopold, *How AI is Reshaping the Career Ladder, and Other Trends in Jobs and Skills on Labour Day*, World Economic Forum, April 30, 2025, https://www.weforum.org/stories/2025/04/ai-jobs-international-workers-day/

V. The Growing Risks Posed by AI in the Financial Sector

The financial sector has long been a proving ground for automation, and complex algorithmic systems. Artificial intelligence now threatens to amplify the sector's long-standing vulnerabilities—opacity, concentration, leverage, and misaligned incentives—while introducing new risks that regulators are only beginning to confront. In finance, small modeling errors, biased decision-making, or runaway automation can rapidly metastasize into systemic instability.[73]

This makes the finance industry's adoption of AI more concerning. In finance, AI systems are no longer peripheral tools. They are increasingly embedded in core functions including[74] but not limited to:

- **Credit underwriting and loan pricing**
- **Fraud detection and transaction monitoring**
- **High-frequency and algorithmic trading**
- **Insurance underwriting and claims processing**
- **Consumer service, collections, and financial advising**
- **Market surveillance and risk management**

These systems shape who gets access to credit, at what price, under what terms, and how adverse decisions may be contested.[75] In short, AI is rapidly becoming a gatekeeper to economic opportunity. Yet many of these systems operate as black boxes, shielded from public scrutiny by trade secrecy, proprietary claims, and technical opacity [76] That dangerous combination threatens transparency, which is the bedrock of trust.

Indeed, the financial industry's enthusiasm for opaque AI systems should raise alarms. This skepticism is well justified by the industry's own historical conduct. This is an industry whose history of redlining, discriminatory lending, and predatory financial products required repeated federal intervention.[77] AI does not erase that history. It threatens to replicate it by operating at an unprecedented scale, speed, and invisibility. AI systems trained on historical data can replicate and intensify past discrimination in credit, insurance, housing finance, and small-business lending.[78] Automated decision systems can deny

---

[73] Hilary J. Allen, *Driverless Finance*, Harvard Business Law Review, https://journals.law.harvard.edu/hblr/wp-content/uploads/sites/87/2020/03/HLB101_crop.pdf
[74] *Id*.; *See also* Gary Gensler, *Chapter 7,* Artificial Intelligence Development and Policy Landscape, December 2, 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5842702 ; *See also* Todd Phillips, *The Risks of Generative AI Agents to Financial Services*, Roosevelt Institute, September 26, 2024, https://rooseveltinstitute.org/publications/the-risks-of-generative-ai-agents-to-financial-services/
[75] *See Id*.
[76] *Id*.
[77] Amalie Zinn et. al., *Building Trust in the Financial System is Key to Closing the Racial Wealth Gap*, Urban Institute, June 15, 2023, https://www.urban.org/urban-wire/building-trust-financial-system-key-closing-racial-wealth-gap
[78] *See supra* note 74.

thousands of applicants in seconds with no clear explanation, no meaningful appeal, and no accountability pathway.[79] Consumers are left with adverse outcomes while firms may claim there is no human decision-maker to confront.[80]

Regulators and researchers have repeatedly documented biased outcomes in automated credit and insurance systems.[81] When discrimination becomes automated, civil rights enforcement must become more robust. Yet the current administration's sustained attacks on civil rights protections threaten to make enforcement nearly impossible precisely when it is most needed.[82]

Beyond consumer harm, AI poses macro-level risks to financial stability. In trading and market-making contexts, machine learning systems react to the same data at the same time, often using similar optimization strategies.[83] That creates the conditions for herding behavior, where large volumes of capital move in lockstep based on similar investor behavior.[84]

History shows how dangerous this can be. High-frequency trading has already contributed to flash crashes and sudden evaporation of liquidity.[85] AI systems, which adapt dynamically and operate at light speed, magnify that instability.[86] When things go wrong, they go wrong faster and at a scale no human intervention can immediately arrest. The central danger therefore is not simply automation. It is automation without explainability, without oversight, and without enforceable guardrails.

AI also introduces a new and underappreciated form of systemic risk: technological concentration. A small number of cloud providers, chip manufacturers, and AI vendors now underpin vast portions of the financial system's digital infrastructure.[87] When those

---

[79] *Id*.
[80] *Id*.
[81] Michael Akinwumi et. al., *AN AI Fair Lending Policy Agenda for the Federal Financial Regulators,* Brookings Institute, December 2, 2021, https://www.brookings.edu/articles/an-ai-fair-lending-policy-agenda-for-the-federal-financial-regulators/
[82] The Leadership Conference on Civil and Human Rights, *Trump Administration Civil and Human Rights Rollbacks*, https://civilrights.org/trump-rollbacks/
[83] *See supra* note 74.
[84] *Id*.
[85] Andrei Kirilenko et. al., *The Flash Crash: The Impact of High Frequency Trading on an Electronic Market*, Commodity Futures Trading Commission, May 5, 2014, https://www.cftc.gov/sites/default/files/idc/groups/public/@economicanalysis/documents/file/oce_flashcrash0314.pdf
[86] Kevin Frazier, *Selling Spirals: Avoiding an AI Flash Crash*, Lawfare, November 8, 2024, https://www.lawfaremedia.org/article/selling-spirals--avoiding-an-ai-flash-crash
[87] Asad Ramzanali, *How to Regulate the Cloud: A Blueprint to Address the Market Failures and National Security Risks of Cloud Computing*, Vanderbilt Policy Accelerator, September 2025, https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2025/09/18140135/How-to-Regulate-the-Cloud.pdf

same firms simultaneously supply compute power, AI models, and financial services platforms, single points of failure multiply across markets.[88]

A rising wave of internet provider outages has made clear how deeply market stability now depends on a handful of infrastructure vendors.[89] As AI deepens this dependence, the resilience of the financial system becomes inseparable from the business incentives of a handful of Big Tech monopolists. This is both a cybersecurity issue and a structural market risk.

The financial system is not just another industry—it is the circulatory system of the economy. When AI distorts that system, the harm does not remain confined to trading floors or balance sheets. It infects households, small businesses, municipalities, and even national and global economies. In finance, experimentation without guardrails historically cost Americans dearly. Chaotic securitization of mortgages, unchecked, led to the housing bubble whose rupture cost millions their jobs, savings, and homes spiraling the nation into the Great Recession.

However, if Congress allows AI to reshape financial markets behind closed doors, without transparency, civil rights enforcement, and systemic risk controls, the price will not be paid only by individual consumers. It will be paid by the stability of the U.S. economy itself. **Public Citizen rejects the notion that Wall Street should be allowed to experiment on the public with diminished accountability. Congress must act with urgency and clarity to prove that democratic governance still has the power to discipline the most powerful sectors of the economy.**

[88] *Id*.
[89] Kevin Collier, *Severe Internet Outages Keep Happening—and They Might Get Worse*, NBC News, November 23, 2025, https://www.nbcnews.com/tech/internet/internet-outages-aws-microsoft-cloudflare-rcna245043

VI. The Mounting Evidence That the United States May Be Entering an AI Investment Bubble

Alongside the rapid deployment of AI across the economy, the United States is witnessing an unprecedented surge of speculative capital flowing into AI infrastructure, startups, and compute supply chains.[90] The sheer scale, speed, and structure of this investment raise a serious and unavoidable question for policymakers: **are we witnessing the early stages of a destabilizing AI investment bubble?**

This is a risk increasingly flagged by economists,[91] market analysts,[92] and even some of the industry's most enthusiastic participants.[93] An economic bubble occurs when asset prices rise far beyond what underlying economic fundamentals can reasonably support. Bubbles are rarely obvious in real time. They are typically characterized by:

- **Unsustainable price growth**
- **Circular financing that inflates apparent demand**
- **Heavy reliance on debt and leverage**
- **Narratives of "this time is different"**[94]

Each of these warning signs is now visible in the AI sector. Unlike traditional public companies, many of the largest AI firms operate behind a veil of limited financial disclosure.[95] As a result, standard valuation metrics, such as price-to-earnings ratios, are often impossible to apply.[96] What is clear, however, is that current AI valuations dramatically exceed what existing revenue, let alone profit, can plausibly justify.[97]

Private market valuations for leading AI firms have reached levels that imply decades of near-perfect execution, exponential productivity gains, and extraordinary profit not

---

[90] Paulo Carvao, *Is AI a Boom or a Bubble?* October 16, 2025, Harvard Business Review, https://hbr.org/2025/10/is-ai-a-boom-or-a-bubble; *See also* Jessica Wong, *Wall Street is Driving the AI Surge. But Millions of Americans Could be in the Blast Zone if the Bubble Bursts*, YahooNews, December 4, 2025, https://finance.yahoo.com/news/wall-street-driving-ai-surge-210000413.html

[91] Thibault Sprilet, *The AI Boom has all 4 Classic Bubble Signs—and it could pop in 2026 if Interest Rates Rise, a Top Economist Says*, Business Insider, December 2, 2025, https://www.businessinsider.com/ai-boom-has-4-bubble-signs-could-burst-2026-economist-2025-12

[92] Eduardo Porter, *The Question isn't Whether the AI Bubble will Burst—But what the Fallout will be*, The Guardian, December 1, 2025, https://www.theguardian.com/technology/2025/dec/01/ai-bubble-us-economy

[93] Dylan Butts, *OpenAI's Sam Altman Sees AI Bubble Forming as Industry Spending Surges,* CNBC News, August 18, 2025, https://www.cnbc.com/2025/08/18/openai-sam-altman-warns-ai-market-is-in-a-bubble.html

[94] *See supra* note 91.

[95] Jacqueline Gu and Cade Metz, *How OpenAI Uses Complex and Circular Deals to Fuel its Multibillion-Dollar Rise*, The New York Times, October 31, 2025, https://www.nytimes.com/interactive/2025/10/31/technology/openai-fundraising-deals.html

[96] Daron Acemoglu, *The Simple Macroeconomics of AI*, MIT, April 5, 2024, https://economics.mit.edu/sites/default/files/2024-04/The%20Simple%20Macroeconomics%20of%20AI.pdf

[97] *Id*.

experienced by any other sector. Yet, as multiple independent studies have shown, the real-world productivity impact of generative AI remains modest, inconsistent, and in many sectors statistically indistinguishable from zero.[98] When valuation growth runs far ahead of demonstrated economic returns, downside risk increases [99]

Perhaps the most troubling structural feature of today's AI economy is the extent of circular financing. In multiple high-profile cases, capital flows from large technology firms and financial conglomerates into AI developers, only to return to those same firms as cloud computing payments, chip purchases, or infrastructure contracts.[100] This creates the illusion of booming external demand when much of the apparent revenue is recycled funding.[101] Circular financing can inflate valuations, obscure underlying market weakness, and mask the extent to which AI firms remain dependent on a narrow set of capital providers.[102] Neighbors who do each other's washing isn't a viable economy. It is a classic ingredient in systemic economic fragility.[103]

Despite extraordinary capital expenditure, leading macroeconomic research suggests that AI's contribution to near-term economic growth is likely to be modest, not revolutionary.[104] Even optimistic estimates project only fractional increases in total factor productivity over the next decade.[105] At the same time, AI-driven gains are expected to flow disproportionately to capital owners, widening inequality between labor and investors.[106] This mismatch between speculative investment and measured productivity is one of the clearest signals of bubble dynamics. Put bluntly: we are spending like a revolution is guaranteed, while the data says it is far from assured.

Another classic bubble indicator now flashing in the AI sector is leverage. Major AI investors have taken on substantial margin loans and bridge financing to sustain their

---

[98] *Id*.; *See also supra* note 94; *See also* Kate Niederhoffer et. al., *AI-Generated "Workslop" is Destroying Productivity,* Harvard Business Review, September 22, 2025, https://hbr.org/2025/09/ai-generated-workslop-is-destroying-productivity; Dritjon Gruda and Brad Aeon, *Seven Myths about AI and Productivity: What the Evidence Really Says*, California Management Review, October 16, 2025, https://cmr.berkeley.edu/2025/10/seven-myths-about-ai-and-productivity-what-the-evidence-really-says/
[99] *See supra* note 96.
[100] *See supra* note 95.
[101] *Id*.
[102] *Id*.
[103] *See supra* note 94.
[104] *See supra* note 99.
[105] *Id*.
[106] *Id*.

capital commitments.[107] When asset prices rise, leverage magnifies gains.[108] When sentiment turns, it magnifies losses and accelerates forced liquidation.[109] This is precisely how localized speculative manias metastasize into broader financial and economic crises. AI's infrastructure buildout is now so large that a sharp contraction would no longer be a niche tech-sector event. It would be macroeconomically meaningful.

The most common historical comparison is the late-1990s dot-com bubble. The parallels include: euphoric narratives, explosive valuations, infrastructure overbuild, and the promise of a productivity revolution just over the horizon.[110] But there is one crucial difference. During the dot-com era, speculative excess was largely concentrated in Silicon Valley equity markets.[111] Today's AI boom is also deeply embedded in physical infrastructure, energy grids, private credit markets, and global supply chains.[112] That suggests that the economic footprint of a potential AI crash could be broader and more painful. Not only would the share price of major public companies spending on AI decline, which could harm worker pension plans, but municipalities helping with data centers or associated power plants might suffer,

It may be tempting for many in Congress to believe in the AI hype. The persistent attempts to pursue federal preemption of state AI regulations suggest that many on Capitol Hill are fully invested. However, one of the most dangerous responses to speculative excess is denial. When governments treat bubble warnings as hostile to "innovation," they amplify the eventual fallout. Smart economic governance does not assume that every boom ends in catastrophe. But it also does not ignore warning signs until markets collapse.

Congress must not regulate AI as if the upside is guaranteed, and the downside is negligible. The downside risks are already visible, and pretending otherwise will only magnify the economic harm. **As speculative risk in the AI sector accelerates, Public Citizen is unequivocal: there must be no AI industry bailout.** Taxpayers must not be turned into the insurer of last resort for reckless corporate overreach. If AI companies truly believe their technology is revolutionary, they should be prepared to bear the full market risk of that claim. **Congress must make this principle explicit now, before instability sets in, not after another crisis forces emergency action. There should be no implicit**

---

[107] Chris Morahan et. al., *AI Funding: The Bull and Bear Investment Case*, Morgan Stanley, December 1, 2025, https://www.morganstanley.com/im/en-us/individual-investor/insights/articles/bull-and-bear-investment-cases.html; Caleb Mutua and Paula Seligson, *Wall Street Races to Cut its Risk from AI's Borrowing Binge*, Bloomberg, December 5, 2025, https://finance.yahoo.com/news/wall-street-races-cut-risk-113000304.html; Nick Lichtenberg, *OpenAI Won't Make Money by 2030 and Still Needs to Come Up with Another $207 Billion to Power its Growth Plans, HSBC Estimates*, Fortune, November 26, 2025, https://fortune.com/2025/11/26/is-openai-profitable-forecast-data-center-200-billion-shortfall-hsbc/

[108] *See supra* note 94.

[109] *Id*.

[110] Jeffrey A. Sonnefeld and Stephen Henriques, *This is How the AI Bubble Bursts*, Yale Insights, October 8, 2025, https://insights.som.yale.edu/insights/this-is-how-the-ai-bubble-bursts

[111] *Id*.

[112] *See supra* notes 94-99.

guarantees, no quiet backstopping of private credit, and no federal assumption of stranded AI infrastructure debt. Losses should remain where they belong: with the investors and executives who chose to take the risk. The American public is not an insurance policy for speculative AI finance.

VII. The "Sandbox" Misnomer and the Broader Deregulatory Strategy

The Senate's SANDBOX Act and Chairman Hill's Unleashing AI Innovation in Financial Services Act are foundational misrepresentations of the term "sandbox." Neither proposal meaningfully resembles a regulatory sandbox. **True sandboxes are narrow, temporary, and tightly supervised environments designed to generate evidence before broader deployment.[113] These bills do the opposite. They use the language of experimentation to justify sweeping, long-term exemptions from existing law, with diminished oversight and heightened risk to the public.** This is not controlled testing. It is preemptive deregulation.

At their core, both bills invert the basic logic of public-interest governance. Instead of requiring companies to demonstrate safety before deployment, they assume safety and force the public to absorb the consequences if that assumption is proven wrong. Instead of strengthening regulatory capacity to meet the scale of emerging risk, they convert regulatory delays and agency under-resourcing into automatic approvals. In both cases, "innovation" becomes the rationale for stripping away the very guardrails that make innovation legitimate. This fits the pattern of Republican's AI deregulatory efforts seen since this summer.

The Senate SANDBOX Act is being marketed as a narrow, innovation-friendly pilot.[114] However, it represents one of the most aggressive deregulatory maneuvers in federal AI policy to date. It would authorize sweeping waivers of federal law for companies deploying AI systems, while simultaneously preempting state protections and sidelining expert regulators.[115] Approval authority would be centralized in an office without enforcement powers, and if agencies fail to act within rigid timelines, approvals would be granted by default.[116] Delay becomes rubber stamped government approval for corporate immunity.

This is not how genuine sandboxes function. Real sandboxes are narrowly scoped, time-limited, regulator-controlled, and designed to inform future safety standards.[117] The SANDBOX Act meets none of those conditions. Its waivers are broad, its duration is long,

---

[113] Lauren Saunders, *Are Fintech Sandboxes a Consumer Protection Desert?* The Hill, November 29, 2018, https://thehill.com/blogs/congress-blog/economy-budget/418770-Are-fintech-sandboxes-a-consumer-protection-desert%3F/

[114] U.S. Senate, *Sen. Cruz Unveils AI Policy Framework to Strengthen American AI Leadership*, Press Release, September 10, 2025, https://www.commerce.senate.gov/2025/9/sen-cruz-unveils-ai-policy-framework-to-strengthen-american-ai-leadership

[115] Senator Ted Cruz, S.B. 2750, https://www.congress.gov/bill/119th-congress/senate-bill/2750/text

[116] *Id*.

[117] *See supra* note 114.

its oversight is diluted, and its regulatory consequences are permanent. It does not test whether systems are safe. It assumes safety and tests the public instead.

The resulting public interest failures are profound. The SANDBOX Act would weaken civil rights and consumer protections, treat people as involuntary test subjects in live-market AI experiments, sideline expert regulators, normalize exemption as the regulatory baseline, and wipe out stronger state protections enacted precisely because Congress has not acted. In short, the SANDBOX Act does not modernize regulations. It obliterates them.

The House bill Unleashing AI Innovation in Financial Services Act follows the same deregulatory blueprint, but confines its experiment to the most systemically sensitive sector of the economy. Under the Act, financial institutions may propose "AI test projects" and seek waivers or modifications of existing rules through "alternative compliance strategies," including rules governing consumer protection, market integrity, and risk management.[118] Once approved, the primary regulator may enforce the waived regulation only through the firm's alternative strategy, and all other financial regulators are explicitly barred from enforcing those same rules.[119] In other words, the supervised entity helps write the terms of its own supervision and then receives statutory protection from the rest of the regulatory system.

The bill hardwires automatic approvals into law. If a regulator fails to act within 120 days, it may extend review once, but after that, inaction becomes approval by operation of law.[120] In an AI landscape defined by opacity and technical complexity, this structure weaponizes regulatory understaffing—particularly in the wake of the Trump administration's mass layoffs—into a built-in deregulatory signoff.

Transparency is also sharply curtailed. Annual reports to Congress may present only *aggregated results* and may not name participating firms.[121] Lawmakers, market participants, and the public will have no way to know which entities were permitted to experiment with high-risk AI systems under relaxed rules or how those experiments affected real consumers and investors. In a sector where trust and stability are paramount, anonymizing experimentation with core financial infrastructure is not responsible governance. It is concealment.

The financial industry's history makes one thing unmistakable: waiting for fraud cases to ripen is regulatory malpractice. Complex AI-driven trading, underwriting, and customer-interaction systems can quietly shift risk, hardwire discrimination, and destabilize markets long before conduct ever meets the narrow legal threshold for emergency intervention. By the time fraud is provable in court, the damage is already done.

These two separate bills represent key aspects of the same deregulatory playbook. This unified deregulatory scheme has appeared repeatedly across legislative vehicles, both

---

[118] Rep. French Hill, H.R. 4801 the Unleashing AI Innovation in Financial Services Act, https://financialservices.house.gov/uploadedfiles/ai_bill.pdf
[119] *Id*.
[120] *Id*.
[121] *Id*.

chambers of Congress, and policy proposals raised by President Trump. Key overlapping concepts include:

- **Strip state authority through preemption.**
- **Fast-track deployment of untested systems.**
- **Centralize power to federal agencies whose leadership has eschewed oversight powers and whose staff have been depleted to create automatic approvals of industry favored laws.**
- **Shift risk downward onto workers, consumers, and communities.**

Under these policy proposals, the public bears the downside while corporations retain the upside. When Congress allows industries to help write their own compliance rules, shields them from scrutiny, anonymizes experimentation on the public, and blocks state governments from responding to local harms, democratic oversight itself becomes collateral damage. **Sandboxes are supposed to be places to experiment while minimizing harm to the public at large.[122] Both the SANDBOX and the Unleashing AI Innovation in Financial Services Act break the very guardrails that make innovation worthy of public trust. They are not experimentation but rather blanket corporate immunity.**

VIII. Guiding Principles for Democratic AI Governance

The choice before Congress is not between innovation and regulation. **It is between unchecked, high-risk deployment that serves a narrow set of corporate interests and responsible, rights-respecting innovation that strengthens the middle class, protects democracy, and preserves financial stability.** The United States can and should lead on AI. But that leadership must be defined by enforceable guardrails that allow the economy to flourish for everyone.

[122] Venkatarangan Thirumalai, *Understanding the Power of AI Sandboxes: A Guide for Beginners*, Founder Catalyst, April 29, 2024, https://thefoundercatalyst.com/2024/04/29/power-of-ai-sandboxes/

A genuinely pro-American AI policy should be grounded in a small set of clear principles:

1. **Human and civil rights are non-negotiable.** AI systems must not be used to discriminate, suppress rights, or evade longstanding civil rights protections. If they do, enforcement mechanisms must be pursued to hold companies accountable.
2. **Accountability follows power.** The more powerful and impactful an AI system is, the stronger and more enforceable its oversight must be. Otherwise, the American public will be vulnerable to one of the most powerful technologies to date and beholden to the interests of a few tech monopolists. Further, corporations cannot be allowed to hide behind machine decisions. If an AI product produces discriminatory, dangerous, or simply injurious results, then the corporations behind that product must bear responsibility.
3. **States remain essential partners.** Federal law should establish a floor of protection, not a ceiling. States must remain free to respond to evolving harms and innovate in the public interest. This represents the will of the American people as shown by consistent polling.
4. **Workers and communities are not collateral damage.** AI policy must prioritize job quality, workplace dignity, and community stability. The American economy was built upon a strong middle class, and Congressional policies must seek to encourage middle class growth.
5. **Financial stability and economic realism matter.** AI cannot be regulated as if its upside is guaranteed, and its downside is someone else's problem. Speculation is not a regulatory strategy, and taxpayers must never be forced to underwrite the consequences of reckless AI finance.
6. **Transparency is the price of public power.** Systems that make or influence decisions about people's rights, livelihoods, or safety must be explainable, contestable, and auditable. This is the bedrock of democratic governance.

These principles are concrete governing standards that must shape legislative text, oversight mandates, and agency rulemaking. They also reflect the core values that have historically allowed the United States to prosper: accountability, fairness, shared prosperity, and democratic control over concentrated power.

Conclusion

Each month that passes without meaningful federal guardrails is another month in which AI systems deepen their footprint in finance, employment, policing, infrastructure, and politics—often under weaker oversight than the industries they are displacing. AI is shaping our society in real time. **The question before Congress is who this technology will serve and who will bear its risks.**

In past eras—whether with tobacco, opioids, financial derivatives, or social media—Congress was told repeatedly to move fast, trust industry, and regulate later. Each time, the public paid the price in lives, livelihoods, and lost trust. AI is moving faster, operating at a greater scale, and concentrating more power than any of those industries ever did. The cost of getting this wrong will be higher.

The United States does not have to choose between leading in AI and leading with values. The only way to do both is through enforceable public-interest guardrails. Congress now has a once-in-a-generation opportunity to decide whether AI becomes another chapter in the story of unchecked corporate power or a model for how democratic societies govern world-changing technologies responsibly.

Public Citizen respectfully submits that the better path forward is not a mystery:

- Reject blanket preemption and deregulatory sandboxes.
- Build enforceable, sector-specific guardrails.
- Invest in regulators' technical capacity.
- Protect workers, children, and communities.
- And refuse to make taxpayers the backstop for speculative AI finance.

This is pro-democracy, pro-worker, pro-consumer, and pro-market stability. It is what serious AI governance looks like. America's leadership in AI will ultimately be measured by whether working families are more secure, markets are more stable, civil rights are protected, and democracy emerges stronger on the other side of this transformation.

That is the standard the public expects. And it is the standard Congress must now meet.