PUBLIC CITIZEN

215 Pennsylvania Avenue, SE • Washington, D.C. 20003 • 202/546-4996 • www.citizen.org

July 16, 2025

Chairman Andy Biggs and Ranking Member Lucy McBath
U.S. House Judiciary Subcommittee on Crime and Federal Government Surveillance
U.S. House of Representatives
2141 Rayburn House Office Building
Washington, D.C. 20515

Re: Public Citizen's Statement for the Record: Artificial Intelligence and Criminal Exploitation: A New Era of Risk

Dear Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee,

Public Citizen appreciates the opportunity to submit this statement for the record for the hearing titled, *Artificial Intelligence and Criminal Exploitation: A New Era of Risk.*[1] As an organization deeply committed to protecting consumers, ensuring corporate accountability, and advancing public-interest technology policy, we have long warned that unregulated artificial intelligence (AI) tools expose consumers to a vast array of harms.[2] Like this subcommittee, we too are concerned about the growing threat of criminal exploitation through AI.

Founded in 1971, Public Citizen is a national nonprofit organization with more than 500,000 members and supporters across the country. We advocate for an accountable government, corporate transparency, and consumer protection in the public interest. Our recent work to support and help pass first-in-the-nation deepfake protections for children at the state level has shown just how urgently policymakers must respond to AI-enabled harms.[3] We advocate for responsible AI guardrails that prevent tech companies from deploying systems that are untested, unsafe, and ripe for abuse. This hearing underscores the importance of this moment in history and the response it demands—swift, enforceable action to protect the public from more sophisticated criminals using AI to effectuate their scams.

[1] *Artificial Intelligence and Criminal Exploitation: A New Era of Risk,* House Judiciary Committee (July 16, 2025), https://judiciary.house.gov/committee-activity/hearings/artificial-intelligence-and-criminal-exploitation-new-era-risk-0.

[2] Rick Claypool, *Chatbots Are Not People: Designed-In Dangers of Human-Like A.I. Systems*, Public Citizen (Sept. 26, 2023), https://www.citizen.org/article/chatbots-are-not-people-dangerous-human-like-anthropomorphic-ai-report/

[3] *Two-Thirds of States Enact Bills Protecting Public from Deepfake Porn*, Public Citizen (May 6, 2025), https://www.citizen.org/news/two-thirds-of-states-enact-bills-protecting-public-from-deepfake-porn/ (last visited July 15, 2025)

I. AI Supercharges Criminal Exploitation

Artificial intelligence now allows criminals to act with speed, scale, and sophistication unimaginable just a few years ago.[4] From phishing emails generated in perfect English to deepfake videos impersonating family members, AI tools are being weaponized in ways that exploit trust, erode safety, and overwhelm law enforcement. In the era of AI a single tool can now produce thousands of personalized phishing attacks or clone a victim's voice in seconds. This proliferation has quickly outpaced previous technology and the models can adapt quickly.

Federal agencies and police departments have raised the alarm. The FBI, in public alerts, has documented an uptick in AI-generated images and videos used to exploit children, extort families, and trick victims into sending money.[5] Local police forces from New York to Los Angeles have similarly warned about a rise in "virtual kidnapping" scams involving cloned voices and AI-generated ransom threats.[6]

One of the most disturbing trends we're seeing involves AI-generated child sexual abuse material (CSAM).[7] In some cases, perpetrators have used deepfake tools to fabricate images of teens and then blackmail them, or their parents, into paying for supposed "deletion."[8] These cases often go unreported due to stigma, shame, or disbelief. Yet the reported cases are growing in number.

As previously mentioned, the concern around AI-generated voice cloning is quickly escalating with more reported examples of voice cloning. Scammers are using AI-generated voice cloning to impersonate family members in distress, pleading for money or bail.[9] In one well-publicized case, a woman in Arizona was requested to send thousands in ransom money by a voice that she believed was her sobbing daughter.[10] These scams are not only heartbreaking, but improvements

[4] *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*, Public Service Announcement No. I-120324-PSA (FBI Internet Crime Complaint Center Dec. 3, 2024), https://www.ic3.gov/PSA/2024/PSA241203

[5] *FBI San Francisco Field Office, 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

[6] *FBI, NYPD Warn of "Virtual Kidnapping" Scam*, CBS New York (Jan. 13, 2015), https://www.cbsnews.com/newyork/news/fbi-nypd-warn-of-virtual-kidnapping-scam/; *LAPD Warning About Virtual Kidnapping Scams in Los Angeles*, NBC Los Angeles, (May 2, 2025), https://www.nbclosangeles.com/news/local/virtual-kidnapping-scammers-targeting-latino-community-los-angeles-lapd/3692425/

[7] *FBI, Charlotte Child Pornography Case Shows 'Unsettling' Reach of AI Imagery*, FBI (Apr. 29, 2024), https://www.fbi.gov/news/stories/charlotte-child-sexual-abuse-material-case-shows-unsettling-reach-of-ai-generated-imagery

[8] *Safeguarding Alert: Sextortion and the Rise of AI*, Safer Schools (July 14, 2025), https://oursaferschools.co.uk/2025/01/20/sextortion-rise-of-ai/; Jacob Knutson, *How AI Is Helping Scammers Target Victims in "Sextortion" Schemes*, Axios (June 23, 2023), https://www.axios.com/2023/06/23/artificial-intelligence-sexual-exploitation-children-technology

[9] Megan Cerullo, *AI Voice Scams Are on the Rise. Here's How to Protect Yourself*, CBS News (Dec. 17, 2024), https://www.cbsnews.com/news/elder-scams-family-safe-word/

[10] GMA Team, *Mom Warns of Hoax Using AI to Clone Daughter's Voice*, ABC News (Apr. 13, 2023), https://abcnews.go.com/GMA/Family/mom-warns-hoax-ai-clone-daughters-voice/story?id=98551351

to AI training are making them increasingly convincing. In short, the public is woefully under protected, while the companies deploying these tools often face no meaningful consequences because there are no federal regulations to hold them accountable.

II. AI Risks Are Real, Yet Some Members Want to Give Big Tech a Pass

The recent backlash to the previously proposed AI moratorium shows the American public are attuned, educated, and following the evolution of AI harms. AI is increasingly woven into our lives and Americans are taking note of the dangers it has already presented, many of which members of this subcommittee are aware of. It is ironic then, if not outright hypocritical, that this hearing is convened to examine the *new era of risk* posed by AI, while some in Congress continue to champion blanket immunity for AI companies under the guise of "innovation."[11]

Congress cannot in good faith acknowledge, as this Subcommittee rightly does today, that AI will supercharge criminal exploitation, and then, in the same Congressional session simultaneously push for proposals like an "AI moratorium," that would prohibit states from enforcing safety and accountability laws for 10 years and that was dangerously close to being included in the recently-passed reconciliation package.[12] Making matters worse, Congress has taken almost no steps to regulate AI and shows no signs of doing so, any time soon. Members cannot with consistency decry AI's growing dangers while refusing to regulate and simultaneously attempting to hand out liability shields to the very companies that have flooded the market with untested, unsafe tools.

To be clear, proponents of this AI moratorium are *absolutely adamant* that freezing any Big Tech accountability is "required" to keep America at the forefront of international competition.[13] U.S. Representative Brett Guthrie has vowed to continue fighting for an AI moratorium that may be less than 10 years.[14] In the Senate, Senator John Thune has stressed that "light touch regulation,"-- his wording for what Public Citizen would call "corporate immunity"-- is the "way to go" on AI regulation.[15] If this hearing is to be taken seriously, one must acknowledge that a moratorium of any length—one month to decades—on state efforts to regulate AI would be recklessly irresponsible given the role that AI plays in criminal objectives to deceive and harm Americans.

AI has become a force multiplier for criminal conduct. This hearing is the very acknowledgement of that. Therefore, members must recall the testimony and statements of the

[11] Mariam Baksh, *Obernolte Says State AI moratorium Would Spur Action on Bipartisan Federal Legislation*, Inside AI Policy (May 22, 2025), https://insideaipolicy.com/ai-daily-news/obernolte-says-state-ai-moratorium-would-spur-action-bipartisan-federal-legislation

[12] Public Citizen, *Senate Votes 99-1 to Remove AI moratorium From Budget in Major Blow to Big Tech and Sen. Cruz*, July 1, 2025, https://www.citizen.org/news/senate-votes-99-1-to-remove-ai-moratorium-from-budget-in-major-blow-to-big-tech-and-sen-cruz.

[13] Colin Wood, *Senate Kills Off Proposed Moratorium on State AI Law Enforcement*, StateScoop (July 1, 2025), https://statescoop.com/state-ai-moratorium-dies-senate/

[14] Diego Areas Munhoz & Ben Brody, *Guthrie Will Keep Fighting for AI Freeze*, Punchbowl News (July 3, 2025), https://punchbowl.news/article/tech/guthrie-ai-freeze-fight/

[15] Ashley Gold & Stefanie W. Kight, *Exclusive: Thune Urges "Light Touch" on AI Regulations*, Axios (June 25, 2025), https://www.axios.com/2025/06/25/thune-ai-moratorium-big-beautiful-bill

record they will see today when Big Tech lobbyists inevitably request a get-out-of-jail-free card through federal legislation and reject any policy that would tie the hands of state and local governments that have taken steps to address the criminal acts made possible through the use of AI.

III. Public Citizen's Recommendations

We urge the Subcommittee—and Congress more broadly—to respond not just with hearings, but with federal legislation. We strongly advocate that Congress:

- **Reject any AI moratorium regardless of length as well as any federal proposal that would preempt stronger state laws.**
- **Pass strong, enforceable AI legislation** that includes product liability, transparency, and safety requirements.
- **Hold AI developers accountable** when their tools are used to commit or enable crimes, especially if those companies have failed to take reasonable safety and risk mitigation steps including, but not limited to, independent third-party audits, incident reports, and safety standards.
- **Demand consumer protection agencies** investigate and respond to AI-enabled scams, fraud, and exploitation.
- **Support law enforcement** in investigating and responding to AI-enabled scams, fraud, and exploitation.

In the hands of bad actors, AI becomes a megaphone for deception and manipulation. Public Citizen stands ready to work with Congress to build an AI policy framework that protects the public, not just corporate bottom lines. As AI reshapes the threat landscape and exposes new ways that criminals can take advantage of unsuspecting consumers, our legal and policy infrastructure must keep pace. Americans deserve no less.

Respectfully submitted,

J.B. Branch
Technology Accountability Advocate
Public Citizen
JBranch@citizen.org