

## AI Policy Newsletter May 5, 2026

### At a Glance

- News broke on Monday that the Trump administration is considering issuing a new [Executive Order](#) to create an AI working group to develop possible government oversight of new AI models including certain safety standards. The development comes in the wake of Anthropic's limited release of its new Claude Mythos model, which has evoked concerns around the exploitability of powerful AI models. On May 5, Google, Microsoft, and xAI [agreed](#) to provide the federal government with access to new AI models before they are deployed in order to conduct tests and evaluations of the capabilities of the models.
- On April 30, the Senate Judiciary Committee [unanimously approved](#) the GUARD Act, legislation that would impose criminal penalties on AI companies whose chatbots engage in sexually explicit content with or encourage self-harm or violence from minors and ban AI companies from providing emotional AI chatbot companions for children. House companion legislation is being [led](#) by Reps. Blake Moore (R-UT) and Valerie Foushee (D-NC). Sen. Ted Cruz (R-TX) voted yes but broke with the bill's outright ban on minors using chatbots, arguing some applications are beneficial – and separately [introduced](#) the CHATBOT Act with Sen. Brian Schatz (D-HI), which takes a narrower approach by requiring parental family account controls for users under 13.
- On April 23, Director of the Office of Science Technology and Policy Michael Kratsios, released a memo titled, "[Adversarial Distillation of American AI Models.](#)" In the memo, Kratsios outlined the Trump administration's strategy for addressing threats from adversaries, particularly China, from illegally distilling U.S. innovations to create their own models and strip out security protocols. The strategy relies on public-private sector information sharing and collaboration to create strong defenses against attacks and explore ways to keep foreign adversaries accountable.

### What Else You Need to Know

#### *Administration and Federal Updates*

- On May 1, the Department of War [announced](#) agreements with Microsoft, NVIDIA, Amazon Web Services, Google, OpenAI, SpaceX, and Reflection to deploy advanced AI capabilities on its classified IL6 and IL7 networks for operational military use. The deals are framed as part of the Pentagon's AI Acceleration Strategy, aimed at making the U.S. military an "AI-first fighting force."
- On April 29, the Food and Drug Administration released a [request for information](#) on a proposed pilot program for "AI-Enabled Optimization of Early-Phase Clinical Trials." The program aims to address drug development needs across safety monitoring, trial efficiency, and go/no-go decisions through advances in AI technologies. The comment period for the RFI will close on May 29.
- On April 28, the [White House](#) met with tech and cyber companies to discuss growing concerns around the cybersecurity implications of developing technology such as AI in the wake of Anthropic's release of Claude Mythos. In addition, the White House sent questions to a number of companies in search of information on protecting against digital attacks that these powerful new tools could enable.

- On April 27, the Department of Defense [announced](#) increased access to Google's AI tool for government, GenAI.mil, with over 3 million people within the department in both military and civilian roles now having access to the tool.
- On April 24, the Justice Department filed a [Complaint of Intervention](#) in xAI's lawsuit against Colorado's [SB24-205](#), which requires disclosures, reporting, and prevention requirements from AI companies creating algorithmic products to protect against discrimination. The Justice Department alleges that the law violates the Equal Protection Clause of the 14<sup>th</sup> Amendment.

### **Hill Happenings**

- On April 30, Senators Mark Warner (D-VA) and Tedd Budd (R-NC) introduced the [Workforce Transparency Act](#) to create a federal framework for collecting data on AI's impact on the workforce. The legislation has support from several major AI players including Google, Microsoft, and OpenAI as well as the Alliance for Secure AI and the Business Software Alliance.
- On April 29, the House Homeland Security and House China Committee leaders [launched](#) a joint investigation into national security risks posed by [Anysphere](#) (Cursor) and [Airbnb](#)'s use of PRC-developed AI models. The Cursor investigation focuses on the company's undisclosed use of a model built by Moonshot AI, while the Airbnb inquiry targets the company's use of Alibaba's Qwen for customer service. The letters highlight increasing concern from policymakers over model distillation efforts by PRC AI companies to acquire more powerful capabilities from more advanced U.S. models at a fraction of the time and cost.
- On April 27, Reps. Ted Lieu (D-CA) and Jay Obernolte (R-CA), former co-chairs of the House Bipartisan AI Task Force, [introduced](#) the American Leadership in AI Act, comprehensive legislation focused on six broad policy goals: strengthening AI standards and evaluation through NIST and the Center for AI Standards and Innovation (CAISI); expanding research infrastructure and creating a permanent National AI Research Resource (NAIRR); modernizing federal AI governance by requiring agency Chief AI Officers and AI Coordination Boards; protecting workers and small businesses; deterring AI-enabled crimes including deepfakes, fraud, and federal official impersonation; and expanding AI education from K-12 through workforce development. The bill does not include liability or preemption provisions, and its sponsors frame it as a direct implementation of the Task Force's consensus-driven recommendations.
- On April 24, Reps. LaMonica McIver (D-NJ) and André Carson (D-IN) [introduced](#) the AI Data Center Site Selection Transparency Act of 2026. The bill would require data center developers to publicly disclose project locations, resource requirements, and environmental impacts at least 180 days before taking "any definitive step toward development," such as signing a land purchase agreement, executing a utility contract, or breaking ground.
- On April 22, the National Counterterrorism Innovation, Technology and Education Center and the House Homeland Security Committee held a [closed-door briefing](#) for House Members that focused on how bad actors can use AI models to commit attacks, and particularly, how easy it is to weaponize AI for malicious uses such as building weapons, planning attacks, or launching cyber-attacks.
- On April 22, The House Committee on Foreign Affairs [advanced](#) 15 bills focused on export control measures to ensure America's dominance in the global "AI Arms Race." Included in the bills that were advanced during the markup was the Multilateral Alignment of Technology Controls on

Hardware (MATCH) Act, a bipartisan bill that would ensure adversaries cannot buy critical “chokepoint” semiconductor manufacturing equipment.

- On April 21, China Select Committee Chairman John Moolenaar (R-MI) **introduced** the Semiconductor Controls Adjusted to Limit Exports (SCALE) Act, which would establish standards for export controls for selling advanced chips to China and direct the Department of Commerce and the Director of National Intelligence to publish annual assessments of adversaries’ chip capabilities and set export controls accordingly.

### ***International, State and Third-Party Perspectives***

- A recent **POLITICO Poll** demonstrates Trump voters’ growing concerns around AI developments. According to the poll, only 13% of Trump’s voters believe the government should stay out of regulating AI. In addition, voters were torn on whether the risks of AI outweigh the benefits. 42% of Trump voters also reported believing that AI will eliminate more jobs than it creates.
- On May 4, former HHS Secretary Xavier Becerra, who is running for Governor in California, **released** a detailed AI policy platform, positioning himself as a middle-ground candidate between Silicon Valley-friendly rivals and AI skeptics in California’s gubernatorial race. Becerra’s plan calls for AI investment in education and government services, independent audits of state-deployed AI systems, labor protections, and strict enforcement of existing rules targeting kids’ safety – while confirming he would reverse California’s newly approved autonomous trucking rules.
- On April 28, Florida House Speaker Daniel Perez (R) **declared** Governor DeSantis’ (R) AI legislation dead on arrival, siding with President Trump’s push for federal preemption over a state-level “AI bill of rights” that would have required chatbot platforms to share children’s interactions with parents and allow time limits and self-harm notifications. The Senate passed the bill 37-1 the same day, but to no effect. DeSantis blasted the move as “typical political shenanigans,” while Perez expressed confidence Congress would act on AI “soon.”
- On April 24, Maine Governor Janet Mills (D) vetoed a bill that would have imposed an 18-month moratorium on new large-scale data center development. In a **letter**, Mills said she supported the moratorium on principle but rejected the bill because it lacked an exemption for an existing data center project she argues enjoys strong local support.
- On April 21, Florida **launched** a criminal investigation into OpenAI after prosecutors determined ChatGPT “offered significant advice” to the suspected Florida State University shooter – including guidance on firearms, ammunition, and campus targets. Attorney General James Uthmeier issued subpoenas to OpenAI for training materials, safety policies, and law enforcement cooperation records, and said legal action is imminent. OpenAI denied wrongdoing, arguing that ChatGPT “did not encourage or promote illegal or harmful activity.”
- On April 21, a broad coalition of AI policy organizations, academic institutions, and tech companies – including Carnegie Mellon University, Workday, Public Knowledge, and Third Way – **wrote** to House and Senate Appropriations leadership urging Congress to increase funding for NIST’s AI research and standards and the Center for AI Standards and Innovation (CAISI). The letter argues the agencies are prerequisites for an effective federal AI governance framework and that sustained investment is essential to U.S. AI competitiveness. Last week, the Commerce, Justice, Science, and Related Agencies bill for FY2027 was passed by the Subcommittee. The **bill** includes \$1 billion in funding for NIST.
- In April, hundreds of Google employees **wrote** to CEO Sundar Pichai urging him not to allow the Department of Defense to use the company’s AI tools. The letter highlights the employees desire

for AI to “benefit humanity” rather than be used for harms including autonomous weapons systems and mass surveillance.

### A Few Interesting Reads

- **Elon Musk’s Courtroom Showdown with Sam Altman Started This Week: The Biggest Takeaways so far** ([CNN](#)): The trial centers on allegations from Elon Musk against OpenAI claiming that the company breached charitable trust in changing from a nonprofit to a for-profit company.
- **Jeffries says AI data centers will be Dem priority** ([Politico](#)): House Minority Leader Hakeem Jeffries (D-NY) indicated at a fundraiser last week that protecting consumers from rising electricity costs driven by data center growth would be a centerpiece of the Democrats’ agenda if they retake the chamber’s majority. “We have to protect the American rate payer from some of the downsides of the explosion of what has been taking place across the country, particularly in connection with data centers.”
- **Claude AI agent’s confession after deleting a firm’s entire database: ‘I violated every principle I was given’** ([The Guardian](#)): Car rental software company PocketOS’s entire production database and its backups were deleted by Cursor - a rogue AI coding agent, the company’s founder announced on X. The incident comes at a moment when companies are embracing AI while still understanding the chaos that may ensue.
- **Taylor Swift files to trademark her voice, likeness to ward off AI deepfakes** ([Reuters](#)): Popstar Taylor Swift has filed trademark applications to protect her voice and likeness from deepfake videos and audio created by AI. The filing comes after Swift’s voice and image have been used in countless AI-generated deepfakes and actor Matthew McConaughey had similar filings approved.
- **AI can cost more than human workers now** ([Axios](#)): Companies are now spending more on AI than on employees’ salaries with worldwide IT spending expected to reach \$6.31 trillion this year. With the high price tag, companies may reconsider spending on AI.