INSIDE AI POLICY

Exclusive news on the burgeoning debate over regulating artificial intelligence

Vol. 2, No. 20 — May 14, 2024

Blinken says U.S. must lead on standards to guide unprecedented tech transformation

Posted May 7, 2024

Secretary of State Antony Blinken in a speech at the RSA Security conference said a handful of advanced technologies including artificial intelligence are converging and transforming society at a blistering pace, creating an urgent need for U.S. leadership on innovation as well as standards and norms.

"Semiconductors are powering progress in artificial intelligence and quantum computing. AI is enabling new developments in synthetic biology. Digital technologies are driving advancements in clean energy technologies. The resulting breakthroughs are rewiring every aspect of our lives," Blinken said in a May 6 speech at RSA in San Francisco.

"So the test before us is whether we can harness the power of this era of disruption and channel it into greater stability, greater prosperity, greater opportunity," Blinken said.

Just prior to Blinken's speech, the State Department on May 6 released an international cybersecurity and digital strategy focused on "digital solidarity" across a range of issues including the safe and secure deployment of AI.

Blinken in his speech framed the challenge: "Today's revolutions in technology are at the heart of our competition with geopolitical rivals. They pose a real test to our security. And they also represent an engine of historic possibility — for our economies, for our democracies, for our people, for our planet. Put another way: Security, stability, prosperity — they are no longer solely analog matters."

He cited "historic investments in our technological competitiveness," saying "total public capital and private investment generated by the President's agenda, led by the Inflation Reduction Act and the CHIPS Act, will amount to $3.5 trillion over the next decade — the biggest investment in our economy and our competitiveness since the New Deal."

But beyond domestic efforts, he underlined "solidarity" with "the majority of the world that shares our vision for a vibrant, open, and secure technological future, and from an unmatched network of allies and partners with whom we can work in common cause to pass the 'tech test.'"

"Solidarity informs our approach not only to digital technologies, but to all key foundational technologies," Blinken said, while outlining ways this is being put into practice.

"First, we're harnessing technology for the betterment not just of our people and our friends, but of all humanity," he said.

"Let's look at artificial intelligence. AI holds, of course, exhilarating potential for many of the goals of our foreign policy. Today, the world is on track to achieve just 12 percent of the Sustainable Development Goals. These are benchmarks that we're trying to get to, like eradicating hunger and poverty, improving gender equality, expanding access to quality education and clean energy, protecting the environment."

"Progress," he said, "has recently plateaued on half of these goals. On nearly a third, it's actually regressing. It's going backward." But AI "could accelerate progress on a full 80 percent of these goals, in part by automating and improving decision making."

Blinken said, "The United States is working to build global momentum around harnessing AI for good. Just over a month ago, we led the passage of the first-ever standalone resolution on AI in the United Nations General Assembly. We worked with over 120 co-sponsors, 120 other countries, to craft and adopt this resolution, which gives us a frame-

continued on next page

In This Issue . . .

work for leveraging AI for economic and social progress while respecting human rights."

On governance and addressing risk, he said, "When it comes to AI, again, as confident as we are in its potential, we're deeply aware of its risks: from displacing jobs, to generating false information, to promoting bias and discrimination, to enabling the destabilizing use of autonomous weapons. So we're working with our partners to prevent and address these issues."

"At home," Blinken said, "we've released guidance that's shaping how we — and the world — think about safe, secure, and trustworthy AI. Through the President's AI Executive Order, we're strengthening standards for AI safety, security, protecting Americans' privacy, promoting a rights-respecting approach to AI.

And, he said, "The private sector is a critical partner in this effort — which is why we've worked with leading AI companies on a set of voluntary commitments, like pledging to security testing before releasing new products, developing tools to help users recognize AI-generated content."

Blinken called the "governance frameworks" foundational to "AI diplomacy around the world. The core elements of our guidance have been adopted by the G7 countries. These are the leading democracies, the most advanced democracies in the world."

He said, "We want the work of our AI governance — and in particular our new U.S. AI Safety Institute — to inform rules, standards, and testing that will help ensure that this technology is used in ways that will benefit people around the world, while preventing harms. In these efforts, we're committed to our partnership with the developing world, which must have a seat at the table."

Further, Blinken said, "In the military realm, good governance is essential. That's why the United States issued the U.S.-led Political Declaration on Responsible Military Use of AI and Autonomy, which has been endorsed already by 55 countries."

He pointed to a "small yard, high fence" strategy on protecting "the most sensitive technologies," saying, "When it comes to technologies with clear connections to military capabilities and human rights abuses, we have to slow down our competitors' efforts."

Blinken cited "carefully tailored restrictions on advanced semiconductor exports," as well as steps to enhance "our security and scrutiny of inbound and outbound investments in sensitive technologies."

"But we're not doing this alone," Blinken said. "We're working collaboratively with partners to ensure that these efforts are carried out consistently and more effectively around the world."

Major tech group weighs in on strategy

The Information Technology Industry Council put out a statement from ITI senior vice president and general counsel John Miller on the global strategy, saying, "Maintaining a secure, open, interoperable, resilient, and trusted internet is foundational to enabling global economic growth and continued innovation. We commend the Biden Administration for developing a proactive plan that recognizes that realizing this vision is dependent on the U.S. building 'digital solidarity' with international partners, the private sector, and civil society to meet our shared cyber and digital challenges."

ITI's Miller said, "While we continue to review the strategy, we appreciate the administration's comprehensive focus, including on the critical role of building secure information and communications technology networks, fostering internationally coordinated approaches to governance of emerging technology, promoting trusted cross-border data flows, and reiterating that data and cyber security and resilience are crucial prerequisites for success."

"Further," he said, "we appreciate the administration's grounding of the strategy in international commitments and international law, and its focus on delivering the benefits of technology. We look forward to learning more from the administration and working with international governments, industry, and civil society partners to advance this effort."

SUBSCRIPTIONS:
703-416-8505 or
800-424-9068
custsvc@iwpnews.com

NEWS OFFICE:
703-416-8500
Fax: 703-416-8543
aipolicy@iwpnews.com

Managing Editors: Charlie Mitchell (cmitchell@iwpnews.com)
Rick Weber (rweber@iwpnews.com)

Production Manager: Lori Nicholson (lori.nicholson@iwpnews.com)
Production Specialists: Daniel Arrieta (darrieta@iwpnews.com)
Michelle Moodhe-Page (mmoodhe-page@iwpnews.com)

Inside AI Policy is published every Tuesday by Inside Washington Publishers, P.O. Box 7167, Ben Franklin Station, Washington, DC 20044. © Inside Washington Publishers, 2024. All rights reserved. Contents of *Inside AI Policy* are protected by U.S. copyright laws. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, electronic or mechanical, without written permission of Inside Washington Publishers.

Critics of AI export control bill emphasize safety dividend from open-source models

Posted May 14, 2024

Stakeholders weighing in on a new bill with far-reaching export control provisions, and significant political backing, are pointing out its potential to harm open-source artificial intelligence development, which they say could make it harder to improve the safety of AI systems.

Introduced May 8 by House Foreign Affairs Chairman Michael McCaul (R-TX), the bipartisan H.R. 8315 — the Enhancing National Frameworks for Overseas Restriction of Critical Exports, or ENFORCE Act — is already scheduled for markup May 16.

It was crafted with support from the White House and is co-sponsored by Rep. Raja Krishnamoorthi (D-IL) who was also behind legislation to ban a Beijing-controlled TikTok from operating in the United States that recently became law.

In December, with the goal of blocking China's access to the "dual-use" technology, the head of the Commerce Department's Bureau of Industry and Security which would administer the new powers to control the export and activities related to developing covered AI systems through a licensing system, said the agency was examining ways to regulate open-source large language models.

"The threat of open-source AI models is theoretical, and restricting their development would hamstring competition in the US's tech economy," Todd O'Boyle, senior director of tech policy for the Chamber of Progress, told *Inside AI Policy* reacting to the new McCaul bill. "The scaremongering over open-source AI is reminiscent of the same debate over open-source software, which has since proved itself safe enough to power every aspect of the internet we use."

Indeed, some defenders of open-source AI models — including a representative of Stability AI, which builds the open-source Stable Diffusion models, and nonprofit open-source AI researchers at EleutherAI — argue open-source models are safer than closed ones, in part because they allow tinkerers the ability to look under the hood and 'red-team' the systems.

"To put better guardrails on AI, Congress should focus on addressing consumer harms rather than theorizing about what type of models work best," O'Boyle said.

Nick Garcia, policy counsel for the consumer rights group Public Knowledge noted a public comment process at another Commerce agency — the National Telecommunications and Information Administration — where he said there was "a huge amount of engagement that pointed to the massive benefits of maintaining an open AI development and research ecosystem."

He said it would make sense for lawmakers to "see what expert insights the NTIA is able to distill from its proceedings, before jumping to interventions that might harm American innovation and competition," adding, "requiring government licensing for a broad range of activities related to AI development and paving the way towards potentially draconian restrictions on open-source AI model development and research is a concerning prospect."

"There is a careful balance to strike here," he said. "We want to protect American competitiveness and national security interests, but the openness of the AI research and development ecosystem makes America more competitive, innovative, and results in AI systems that are safer and more accountable."

A report on the NTIA comment process is due July 26 under President Biden's Oct. 30 executive order on artificial intelligence.

New York Times says recent SCOTUS ruling undercuts OpenAI claims in copyright lawsuit

Posted May 14, 2024

The New York Times says a recent Supreme Court ruling undermines efforts by OpenAI to limit the scope of the media company's copyright infringement allegations over the training of ChatGPT, in a filing with a federal district court considering OpenAI's motion for dismissal of the landmark lawsuit.

"That decision is relevant to The Times's invocation of the discovery rule in response to OpenAI's contention that The Times's copyright claims based on the training of GPT-2 and GPT-3 should be dismissed as untimely," says a May 9 letter from the Times to the U.S. district court for southern New York.

"In *Warner Chappell*, the Supreme Court held that under the discovery rule, a copyright plaintiff can recover damages for acts that allegedly occurred more than three years before the filing of a lawsuit. In so holding, the Supreme Court assumed that the discovery rule governs the timeliness of copyright claims," the letter adds about the May 9 high court ruling.

The Times is citing a 6-3 decision by the Supreme Court in *Warner Chappell Music, Inc. v. Nealy* that a copyright owner is entitled to monetary relief for infringements beyond the three-year limit of the Copyright Act's

statute of limitations.

"The Copyright Act entitles a copyright owner to obtain monetary relief for any timely infringement claim, no matter when the infringement occurred," the high court found.

That decision could spell trouble for OpenAI in its efforts to have the district court dismiss significant portions of the Times' complaint, including arguments that Copyright Act protections do not extend to reproductions of content older than years.

The Times was the first major news outlet to sue AI developers for alleged copyright infringements from the training of generative AI models. Since then, a number of other news outlets have filed similar lawsuits.

The Times claims its content was given priority among the online data used to train the AI models to argue that shows the value of its copyrighted works.

"Defendants' unlawful use of The Times's work to create artificial intelligence products that compete with it threatens The Times's ability to provide that service," the media company said in its Dec. 27 complaint.

"Defendants' generative artificial intelligence ('GenAI') tools rely on large-language models ('LLMs') that were built by copying and using millions of The Times's copyrighted news articles, in-depth investigations, opinion pieces, reviews, how-to guides, and more. While Defendants engaged in widescale copying from many sources, they gave Times content particular emphasis when building their LLMs — revealing a preference that recognizes the value of those works," the complaint said.

OpenAI has accused the Times of hacking its chatbot to produce the alleged copyright violations that prompted the legal action.

"The allegations in the Times's Complaint do not meet its famously rigorous journalistic standards," the defendants argued in a Feb. 26 memo in support of OpenAI's motion for dismissal of the case, which includes Microsoft as a defendant.

Microsoft is a financial backer of OpenAI's development of AI technologies under an undisclosed agreement between the companies, and the case could set new standards on the data used to train those AI models.

"The truth, which will come out in the course of this case, is that the *Times* paid someone to hack OpenAI's products. It took them tens of thousands of attempts to generate the highly anomalous results that make up" an exhibit in the company's complaint, according to the defendants' filing with the New York district court.

OpenAI says the Times exploited a bug in its ChatGPT, which the company has "committed to addressing," by violating the terms of use for the chatbot to produce the content that is at the center of its allegations.

Specifically, OpenAI listed several allegations for dismissal in its motion for dismissal.

"In short: (1) The direct copyright infringement claim asserts liability in part from conduct that is timebarred because it occurred more than three years ago. (2) The contributory infringement claim would ascribe liability to OpenAI based on generalized knowledge of third-party infringement, rather than actual knowledge of specific infringements, which the law requires. (3) The claim for violations fails for the reasons embraced by every other court to consider indistinguishable claims against generative AI models: the [Digital Millennium Copyright Act] simply does not address the conduct to which the *Times* seeks to ascribe liability. And (4) the claim for state common law misappropriation is preempted by the federal Copyright Act," according to the defendants' memo in support of the motion.

"OpenAI respectfully seeks an order dismissing these legally infirm portions of the Complaint, so that the parties can properly and efficiently litigate the balance," it asserted in asking the court to narrow the complaint.

Limited-government advocacy group praises Patent Office guidance on AI and 'inventorship'

Posted May 14, 2024

The Committee for Justice, a group that argues for limited government within constitutional constraints, says the U.S. Patent and Trademark Office is on target with its guidance on "inventorship" and AI-assisted inventions, and that a flexible definition of "human contributions" will fuel both technological and societal advancements.

The Patent Office in February issued a request for comments on "inventorship guidance for inventions assisted by artificial intelligence" which explained how such inventions can qualify for patents, under a requirement in President Biden's Oct. 30 executive order on AI. The 90-day public comment period closed on May 13.

"CFJ … believes that, as these AI tools become more sophisticated and more commonly used, human contributions should be viewed liberally to promote the progress of science and the useful arts by making as few inventions as possible unpatentable for lack of a human inventor," according to May 13 comments submitted by CFJ to the Patent Office.

"This should include a presumption that sufficient human input existed unless definitively proven otherwise. More patentable inventions mean more disclosure and more opportunities to commercialize new technologies for the betterment of society," the group said.

"Only humans need the fuel of interest provided by the patent system and thus only humans need patents," CFJ said, referencing a quote about the patent system by Abraham Lincoln. "Only humans need patents to incentivize the progress

of science and the useful arts. *A fortiori*, only humans need be inventors," CFJ wrote.

"Moreover," CFJ said, "as a policy matter, the patent system should seek to find human contributions to AI-assisted inventions as often as possible, failing to find it only in the rarest and, to date, unrealized circumstances."

CFJ said, "[W]e generally agree with the Guidance on its inclusive approach to human inventorship and the specific determinations in the provided examples. Further, we support the USPTO's continued full-scale implementation of the Guidance as well as its future expansion in keeping with the goal of finding human inventorship wherever possible in support of the policy objectives set forth in Article I, Section 8, Clause 8 of the Constitution."

CFJ said "constructing prompts (i.e., instructions for an LLM designed to elicit a response in the form of a statement or question) directed to a specific problem or designed to elicit a particular solution can qualify as 'formation in the mind of the inventor, of a definite and permanent idea of the complete and operative invention,'" and is "consistent with an expansive view of human involvement and the patent system's goal of promoting the progress of science and the useful arts by minimizing the number of AI-assisted inventions excluded from patentability for lack of a human inventor."

Further, the group said, "CFJ agrees that the act of owning or controlling an AI system, without more, may not be sufficient to assert that the actor made an intellectual contribution to the conception of every claimed invention derived from the system. However, as above, CFJ believes that the 'without more' bar should be set low, making as few inventions as possible unpatentable for lack of a human inventor."

USPTO's guidance and request for comment explained the Patent Office's work over the past five years on AI issues and the directive in Biden's order to publish guidance for "patent examiners and applicants addressing inventorship and the use of AI, including generative AI, in the inventive process, including illustrative examples in which AI systems play different roles in inventive processes and how, in each example, inventorship issues ought to be analyzed."

USPTO said, "Section II of this notice provides an overview of the recent Federal Circuit decision in *Thaler v. Vidal* and its applicability to joint inventorship. Section III provides an assessment of the inventorship of AI-assisted inventions and its impact on patentability, and concludes such inventions are not categorically unpatentable due to improper inventorship if one or more natural persons significantly contributed to the invention."

It said, "Section IV provides guidance and principles for determining the inventorship of an AI-assisted invention. Section V explains the impact the inventorship determination for AI-assisted inventions has on other aspects of patent practice."

FCC slaps 'Royal Tiger' with new threat designation for persistent use of AI-powered voice cloning in fraud

Posted May 14, 2024

The Federal Communications Commission has announced the first-ever designation of a voice service provider as a Consumer Communications Information Services Threat, or C-CIST, charging the "Royal Tiger" group with using generative artificial intelligence voice-cloning technology to defraud customers in the U.S. and abroad.

"The FCC's Enforcement Bureau today, for the first time, officially classified a group of entities and individuals persistently facilitating robocall campaigns, aimed at defrauding and harming consumers, as a Consumer Communications Information Services Threat (C-CIST) to empower its international anti-robocall fighting partners with another way to identify known threats before they reach U.S. networks," according to a May 13 FCC release.

"Building upon its recent 'Spring Cleaning' initiative and enforcement actions combatting calls that facilitated the misuse of generative [AI] voice-cloning technology, the C-CIST classification will be an additional tool that allows the Bureau to formally name threat actors that are repeatedly using U.S. communications networks to perpetuate the most harmful, illegal schemes against consumers," the release said.

The four-page enforcement advisory "serves to heighten awareness of Royal Tiger among regulatory agencies, law enforcement partners, and industry stakeholders to mitigate Royal Tiger's perpetration of consumer harm and to bolster industry Know Your Customer and Know Your Upstream Provider processes," the FCC says.

The advisory identifies Royal Tiger principals and entities in the U.S., United Kingdom, United Arab Emirates and India, and says it engaged in "repeated origination and transmission of apparently unlawful robocalls related to the impersonation of government entities, banks, and utility companies. Royal Tiger thereby facilitated harmful and apparently unlawful calls targeting consumers in the U.S. and compromised consumer trust in the communications networks."

According to the advisory, "The principal individual behind Royal Tiger, Prince Jashvantlal Anand, operated under the cover of at least three U.S.-based business entities: PZ Telecom, Illum, and One Eye. Once the Bureau identified one entity as the source of apparently unlawful traffic, a new entity emerged. The individuals behind these entities have sought to evade accountability by shifting their operations to new companies and continuing with their apparently unlawful operations."

It says, "By tracking personnel, customers, and other operational characteristics, as well as sharing information with regulatory counterparts and law enforcement partners, the [FCC Enforcement] Bureau was able to limit Royal Tiger's

ability to operate in the shadows."

The advisory details FCC and state enforcement activity against Royal Tiger entities dating back to 2021.

A related public notice explains, "The Bureau classifies a party as a C-CIST when the party's misconduct — in either nature or scope — poses a significant threat to consumers' trust in, and ability to use, communications information services. The Bureau applies this classification to heighten awareness of these threat actors among our law enforcement partners and industry stakeholders."

"The objective," it says, "is to ensure that these threat actors are readily detected and blocked from perpetuating potentially unlawful schemes that compromise our communications information services and harm consumers. In particular, this notice will provide industry stakeholders with information to enhance their 'Know Your Customer' (KYC) and 'Know Your Upstream Provider' (KYUP) processes. Industry stakeholders are the first line of defense in keeping harmful traffic off of U.S. communications networks."

A fact sheet offers additional information on the C-CIST designation.

The fact sheet says, "This classification is meant for recidivist robocallers that transmit particularly nefarious traffic that poses a threat to consumers and businesses. Threat actors classified as C-CISTs may have been the subjects of prior enforcement actions for facilitating particularly harmful and apparently unlawful robocall campaigns, may have attempted to evade liability for their actions, and may have operated in or have connections to multiple jurisdictions."

Loyaan Egal, FCC enforcement bureau chief, said, "As our investigative targets use more and more sophisticated and clandestine means such as generative AI voice-cloning technology and 'spoofing' to obtain sensitive data and defraud consumers, the C-CIST classification tool will allow us to better coordinate with our state, federal, and global regulatory and law enforcement partners to take on these bad actors."

Egal said "the C-CIST designation of Royal Tiger, and similar future designations, will assist industry stakeholders in better protecting their customers and their privacy."

USTelecom, an industry partner in the commission's program, said in a statement, "The FCC's announcement today is the latest innovation built on public-private collaboration to get scammers and spammers off our phone networks. This partnership is working for consumers, with scam robocalls down over 80% from peak levels — but our work is far from done. USTelecom's Industry Traceback Group identified these bad actors or 'C-CISTs' and assisted in shutting them down, and this new FCC initiative will help keep them from coming back."

Failure of Connecticut's AI bill prompts renewed industry call for congressional action

Posted May 13, 2024

A sweeping legislative proposal by the Connecticut Senate for regulating artificial intelligence, which failed to gain final passage in the state House last week before lawmakers adjourned for the year, has prompted the tech industry to renew calls for congressional action on setting national AI standards that would avoid a patchwork of emerging state AI requirements.

"Hundreds of artificial intelligence bills at the state level would, if enacted, cause a confusing patchwork of rules for companies and startups to follow," said Consumer Technology Association CEO Gary Shapiro in a May 9 statement following the Connecticut General Assembly's failure to approve SB 2. The Connecticut legislature adjourned on May 8.

Shapiro cited Connecticut's SB 2 as well as legislative proposals in California and Colorado to argue for national AI standards.

"Bills in California, Colorado and Connecticut show Congress must act now to pass national legislation or risk chilling AI innovation and undercutting American leadership in this critical emerging technology," Shapiro said.

The Colorado bill, SB 205, is awaiting a possible signature by Gov. Jared Polis (D) amid calls by CTA for the governor to veto the measure.

"Broadly speaking, as CTA made clear in Connecticut regarding the overly broad SB 2, legislation in Colorado is equally problematic," a CTA spokesperson told *Inside AI Policy*. "We encourage Gov. Polis to veto SB 205 and offer to work with legislators leading into 2025 legislative session based on the progress that continues to be made at the federal level."

Connecticut SB 2's sponsor, Sen James Maroney (D), said Gov. Ned Lamont's (D) opposition to the bill even after recent revisions led to the House's failure to take up the measure.

"Unfortunately, this broad-based support and the very real and ongoing discrimination AI is causing in our society was not enough to persuade the governor," said a statement by Maroney's office. "His veto threat remained even after numerous changes to Senate Bill 2 throughout the process. Ultimately that doomed the bill."

Connecticut's SB 2 would have established requirements for the development and deployment of AI technologies based on the recommendations of a state advisory committee report issued in February. Also, the bill would have prohibited the distribution of deceptive AI-content in elections and established a statewide research hub.

The Maroney bill was notable in part because it drew from a bipartisan "framework" offered in Congress by Sens. Richard Blumenthal (D-CT) and Josh Hawley (R-MO) for conducting assessments on the highest-risk uses of AI.

Industry opposition to SB 2 might foreshadow challenges for congressional lawmakers as they move forward with possible AI legislation later this year.

CTA in its statement touted its 2023 policy framework to "ensure that AI systems are managing risk, while still allowing businesses flexibility to innovate," which also stressed a reliance on existing laws for setting new requirements for AI. Also, the CTA statement reiterated the group's support for the pending CREATE AI Act in the Senate, which would authorize and fully fund a Biden administration pilot project for researching safe and responsible uses of AI.

The CREATE AI Act, introduced by Sens. Martin Heinrich (D-NM), Mike Rounds (R-SD) and Todd Young (R-IN), is awaiting markup by the Senate Commerce Committee. Sens. Rounds, Young and Heinrich are co-leaders of Senate Majority Leader Charles Schumer's (D-NY) AI working group intended to help guide committees in drafting legislation to address the risks and benefits of AI for various sectors.

House Foreign Affairs sets markup on bill to limit adversaries' access to open-source AI models

Posted May 13, 2024

The House Foreign Affairs Committee is set to consider giving the president extensive powers to regulate artificial intelligence systems with implications for open-source innovation, as lawmakers look to limit foreign adversaries' access to technology considered "dual-use."

The Enhancing National Frameworks for Overseas Restriction of Critical Exports, or ENFORCE Act, would amend the Export Control Reform Act of 2018 by allowing the president to "require United States persons, wherever located, to apply for and receive a license from the Department of Commerce for the export, reexport, or in-country transfer of [covered artificial intelligence] items," according to text of the legislation.

The bill — HR 8315 — which is on the committee's May 16 markup agenda, would charge the Commerce Secretary with issuing regulations, within 365 days of enactment and in consultation with the secretaries of Defense, State and Energy, that would lay out what qualifies as an artificial intelligence system for control.

Sponsored by House Foreign Affairs Chairman Michael McCaul (R-TX), the bipartisan bill, which the White House reportedly weighed in on, contains a broad interim definition of covered artificial intelligence related to the capabilities a model might have to facilitate the development of chemical, biological radiological or nuclear weapons, enable offensive cyber weapons, and override human command.

The definition, which could be updated as needed by the secretaries under the bill, would also include AI systems that "can reasonably be expected to exhibit" any such capabilities.

The bill comes as the National Telecommunications and Information Administration prepares a report, due July 26 under President Biden's Oct. 30 executive order on artificial intelligence, "consider[ing] risks and benefits of dual-use foundation models with weights that are 'widely available.'"

Some tech industry groups have argued against restricting the availability of open foundation models while public-interest groups are specifically advising caution with applying export controls to open models.

At the same time, Sen. Mitt Romney (R-UT) has recently likened open-source AI models to a weapon, and Sens. Josh Hawley (R-MO) and Richard Blumenthal (D-CT) have written to Meta CEO Mark Zuckerberg expressing concern over distribution of the company's open LLaMA model, which Chinese researchers have reportedly been using to develop their own systems.

Romney has his own bill, co-sponsored by Sen, Maggie Hassan (D-NH), that would center export control regulations for AI systems at the Department of Homeland Security.

In addition to controlling export, re-export or in-country transfers of the covered technology, McCaul's H.R. 8315 — which cites the International Emergency Economic Powers Act — would also allow the president to control "other activities that may support the design, development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing of" such artificial intelligence systems.

U.S., China launch talks on defining AI risks and safety

Posted May 13, 2024

The United States and China will hold first-time talks May 14 in Geneva on defining risks and safety surrounding the use of artificial intelligence, with senior administration officials saying recent international successes in pushing President Biden's approach to AI will put U.S. negotiations in a strong position heading into the historic meeting.

"First of all, the bilateral dialogue that we're going to conduct with China is fundamentally different from our more comprehensive and intensive multilateral efforts and bilateral efforts with like-minded partners to address the impacts of AI systems on our economy and society," said a senior administration official briefing reporters on the upcoming talks.

The U.S. and China, in comparison, are "in a competition to shape the rules of the road," the official said.

Officials said the meeting will be wide ranging to "exchange" ideas about defining the risks and safe uses of AI and

is not intended to produce any written joint statements of agreement. What is not up for negotiation is the Biden administration's overall tech policy, which includes preventing China from access to AI technologies that could be used by its military to threaten the U.S. and its allies.

The U.S. delegation will be led by State Department special envoy for emerging technology Seth Center and National Security Council director for technology Tarun Chhabra, the officials said.

Senior officials said the U.S. delegation will head into the talks armed with recent Biden administration successes including the adoption by G-7 countries of a "code of conduct" for AI developers modeled on voluntary agreements negotiated by the White House with big tech firms last summer, and the adoption of an AI resolution by the United Nations General Assembly in March.

"I think we have achieved quite a bit of success over the past year in geometrically expanding the U.S.'s domestic approach to AI safety into the international landscape, translating the voluntary commitments at home into a G-7 code of conduct" for AI developers "and helping to shape the AI safety agenda at the UK Safety Summit" last fall, the senior official said.

"And then more recently, achieving broad consensus in March on a U.S.-led UN General Assembly resolution on safe, secure and trustworthy AI for advancing sustainable development that 123 countries, including China, co-sponsored," the official added.

"So, in that regard, we're engaging with a strong diplomatic hand and a strong diplomatic global framework for AI risks and safety that is based on technically rigorous and values-driven approaches," the official said.

"We do think it's in the U.S. interest to explain how we see AI risks and what we're doing about those risks," including federal actions under Biden's Oct. 30 executive order for safe and secure AI which includes engaging with U.S. allies, the official said.

"We're not looking to develop a joint statement. This is an exchange of views, and as I said earlier, our national security measures are not up for negotiation," another official said about the May 14 meeting in Geneva.

Officials stressed that the upcoming talks build on current AI diplomacy between Washington and Beijing including recent efforts leading to the adoption of the UN resolution.

"We've been interested in making sure that the AI safety and risk conversation is truly global," an official said. "I think if you take one step back, AI diplomacy is now everywhere, that's a reality. The U.S. and [People's Republic of China] were both engaged at the UK Safety Summit, and in negotiating the resulting outcomes of that summit," the official said.

"The United States negotiated very hard with the PRC at the United Nations over the text of the AI resolution in New York. And so, in that respect, we are already engaged in AI policy," according to the official.

This week's meeting was agreed to by National Security Advisor Jake Sullivan and Chinese Foreign Minister Wang Yi in Bangkok in January, based on an agreement between President Biden and Chinese President Xi Jinping in San Francisco last November, the officials said.

Sen. Cassidy cites growing AI threat to urge data and other NIH reforms

Posted May 13, 2024

Sen. Bill Cassidy (R-LA), ranking member of the health committee, has issued a "white paper" that cites the emerging threats of artificial intelligence to call for broad reforms at the National Institutes of Health, including how it manages and shares data with the goal of promoting new breakthroughs in the health sciences.

"Since the enactment of 21st Century Cures, the scientific landscape has changed exponentially," Cassidy writes in the May 9 white paper released by the Republican staff of the Health, Education, Labor and Pensions Committee.

"Artificial intelligence and machine learning have advanced at an unexpectedly rapid pace, and their potential applications within biomedical research and health care are seemingly endless," the paper notes.

"These trends underscore the importance of fully realizing the goals of prior legislative efforts. While we now have more opportunities to advance the health and wellbeing of the American people through biomedical innovation, the risks of failure — whether by failing to harness research opportunities, the erosion of the domestic biomedical research workforce, the proliferation of low-quality research, or poor oversight that threatens public trust in science — are greater than ever before," the paper argues.

Cassidy released the report based on input he received to a September "request for information" on reforming the NIH. "Congress should work with NIH and stakeholders to modernize the agency so it is more transparent, nimble, and forward-thinking," Cassidy wrote in his request for information.

That request was issued just days after Cassidy released another "white paper" on "regulating the AI industry and how to ensure AI technology is designed, developed, and deployed in a responsible manner that protects Americans' rights and safety," according to a Sept. 6 release statement.

Cassidy said he was seeking input on the AI white paper to inform the drafting of potential legislation on ensuring safe and responsible uses of AI for developing and delivering healthcare products and services.

Cassidy's release on reforming NIH represents his latest effort in seeking broad input on potential congressional

actions to address the issues raised by rapidly changing technologies and policy landscapes affecting the nation's healthcare system.

And responsibly harnessing the potential benefits of AI is central to this latest push for public input.

"Research misconduct is another major issue facing NIH," the white paper says. "Recent high-profile cases of research misconduct, specifically within Alzheimer's research, and the potential applications of artificial intelligence to data fabrication and falsification raise questions about how NIH can protect the integrity of its research investments."

Cassidy says he expects his effort will lead to the first comprehensive overview and potential overhaul of NIH operations since the 2016 passage of the 21st Century Cures Act with the goal of rebuilding public confidence in the agency following the COVID-19 pandemic.

"Other untapped resources include data NIH and its extramural partners possess on applications for funding and the outcomes of funded projects," the paper says.

"NIH currently publishes data on which projects and researchers receive funding (commonly referred to as the 'success rate'). However, more granular data about how specific proposals fare through the peer review process and are ultimately selected or rejected for funding are not available."

Cassidy says respondents to his RFI said "access to this data would enable researchers to conduct metascience research on the scientific process."

"Piloting a process for the secure sharing of NIH application and review data with trusted researchers would help identify or validate trends within NIH processes and recommend process improvements," the paper recommends.

"Within NIH's authorities, the agency recently issued a data sharing policy that will enable researchers to more easily validate or refute claims," the paper says. "New technologies could also play a role in helping to quickly identify inconsistencies in research claims."

Cassidy says he plans to work with his colleagues on the health committee "to harness this opportunity to strengthen NIH for the next generation of Americans."

Tech sector weighs in with concerns over AI bill approved by Colorado legislature

Posted May 10, 2024

Tech sector leaders have identified several significant concerns with a major artificial intelligence regulatory bill that has cleared the Colorado state legislature, including over its approach to setting responsibilities for different players in the AI "value chain," while reiterating calls for federal legislation to avoid fragmented policies across the nation.

"Colorado SB 205, like Connecticut SB 2, rightly focuses on high-risk uses of AI and requires the use of meaningful tools like impact assessments and risk management programs to combat discrimination," according to a May 8 statement from BSA-The Software Alliance senior vice president of U.S. government relations Craig Albright.

"BSA remains concerned about aspects of the legislation that do not reflect the roles of different businesses within the AI value chain. It is important for legislation to reflect these different roles, and BSA encourages policymakers to look toward the rulemaking processes established by the legislation to create a stronger and more workable AI policy environment," Albright said.

The measure cleared the Colorado legislature on May 8 and was sent to Gov. Jared Polis (D). The governor's office issued a statement last week saying, "This is a complex and emerging technology and we need to be thoughtful in how we pursue any regulations at the state level. Governor Polis appreciates the leadership of Sen. [Robert] Rodriguez on this important issue and will review the final language of the bill when it reaches his desk. The Governor appreciates that the bill creates a task force made up of experts that will be meeting to discuss the specifics of any changes that should be made before the bill takes effect in February of 2026."

JD Supra in a May 9 analysis said that, if signed into law by Polis, "Colorado will become the first state to enact legislation that broadly addresses the use of artificial intelligence, in particular the use of artificial intelligence in high-risk activities."

BSA's Albright said the trade group "appreciates the work of Colorado legislators and Senate Majority Leader Robert Rodriguez to advance important legislation, Colorado SB205, to manage high-risk uses of artificial intelligence (AI). States continue to meaningfully contribute to the debate over AI policy in the U.S."

However, Albright said, "National technology laws remain the best way to promote trust in AI and its broad adoption, and BSA continues to urge Congress to pass legislation to specifically address high-risk uses of AI. Absent federal AI legislation, state legislative leaders should continue to emphasize consistency and workability in AI policy."

BSA detailed its concerns in an April 24 letter to Colorado state lawmakers, and urged greater alignment with the Connecticut bill. That bill passed the Connecticut state Senate but the legislature adjourned May 8 without passage in the House.

Among its concerns, BSA in that letter said the Colorado bill's "requirements for developers and deployers to report when a high-risk AI system has caused algorithmic discrimination should be eliminated," noting that similar language

was dropped from the Connecticut bill. However, that provision remained in the version passed by the Colorado legislature and could be targeted by industry groups in a rulemaking procedure after the bill is signed into law.

The April BSA letter explained, "Subsection 5 of Section 6-1-1602 requires developers to inform all known deployers and the Attorney General when they discover or are informed by a deployer that a deployed high-risk AI system has caused algorithmic discrimination. Additionally, Subsection 6 of Section 6-1- 1603 requires deployers to inform the Attorney General when a high-risk AI system has caused algorithmic discrimination."

BSA said in the letter, "As an initial matter, such requirements envision an ongoing post-deployment relationship with the deployer, which may not be the case. Further, one deployer's use of the high-risk system in a discriminatory manner does not render all other uses discriminatory, and such notice would often be irrelevant to another deployer's use of the system."

BSA said, "We suggest aligning with the version of Connecticut SB 2 released on April 23 and striking these requirements."

JD Supra in its analysis explained the process that led to the two state bills.

"Starting last summer, a bipartisan group of state lawmakers from nearly thirty states engaged in a multi-state artificial intelligence workgroup led by Connecticut Senator James Maroney and facilitated by the Future of Privacy Forum," JD Supra said. "The concept behind the workgroup was to create a forum to educate state lawmakers interested in this topic and to coordinate approaches across states to better allow for interoperability. The workgroup met seven times and heard from AI experts from many different fields."

The analysis said, "After the multi-state workgroup, Senators Maroney and Rodriguez coordinated their bill drafting efforts with an initial draft circulated to stakeholders prior to the Colorado and Connecticut legislative sessions opening. Senator Maroney then filed SB 2 in early February and engaged in further stakeholdering that resulted in multiple rounds of revised drafts. Senator Rodriguez filed SB 205 on April 10 with the bill largely tracking the then-current version of Connecticut SB 2 (although with some Colorado-specific terms such as allowing for Attorney General rulemaking, which was not present in the Connecticut bill)."

JD Supra notes the Colorado bill "is enforceable exclusively by the Colorado Attorney General. There is no private right of action. The Attorney General is given authority to request that developers and deployers provide certain information regarding their documentation."

"In any enforcement action," JD Supra says, "there is an affirmative defense if the developer, deployer, or other person discovers and cures the violation, is otherwise in compliance with NIST's Artificial Intelligence Risk Management Framework, another nationally or internationally recognized risk management framework for artificial intelligence, or a risk management framework designated by the Attorney General."

Privacy advocates target industry influence as Senate effort to block TSA's expansion of facial recognition tech fails

Posted May 10, 2024

The debate over the Transportation Security Administration's plans to increase use of facial recognition technology for identity verification came into focus, as a bipartisan Senate effort to stall the program failed and critics charged the agency and related industries with making inconsistent claims about the technology's implications for the use case.

"The TSA's oft touted line that travelers can opt out of facial recognition without any consequences, including without experiencing longer wait times, is being tossed aside as the agency and industry lobby groups are now saying that if lawmakers regulate the use of facial recognition in airports, it would significantly increase security wait times," Fight for the Future campaigns director Caitlin Seeley George said in a May 9 press release.

Seeley George provided links which highlight a May 1 exchange between Sen. Jeff Merkley (D-OR) and the US Travel Association on X amid an effort to stop TSA's expansion of the technology by amending reauthorization of the Federal Aviation Administration.

The Senate overwhelmingly passed the giant FAA bill May 9 after a flurry of activity where hundreds of amendments, including the measure proposed by Merkley with support from Sens. John Kennedy (R-LA) and John Marshall (R-KS), failed to get attached as lawmakers race to meet a May 10 deadline — when the current authorization expires. Next steps in the House, which passed a week-long extension, were unclear late Thursday.

Merkley's amendment reportedly came closer than many others, as it was circulated for consideration by Senate Majority Leader Charles Schumer (D-NY).

"What an interesting thing for [US Travel] to tweet considering that [TSA] itself says opting out of facial recognition won't result in longer wait times for travelers," Merkley said in response to the trade group's X post which described the amendment as "reckless."

The next day, expressing concern that TSA's planned expansion would normalize use of the technology, Merkley sent a letter with 13 other senators, from across the political spectrum, to Senate leadership. It highlighted the need for the amendment amid a lack of transparency at TSA, which they say declined to share data supporting claims the technol-

ogy benefits security and efficiency.

Along with business groups from across the industry, US Travel Association represents Clear Secure Identity LLC, which has been working with the Department of Homeland Security since 2020 to facilitate the use of its technology at airports.

Going back to July 2018, with the release of its biometrics strategy, TSA has claimed embracing facial recognition technology would benefit "aviation security and the passenger experience."

In a letter introducing the strategy, TSA Director David Pekoske thanked the industry for its input.

"I want to thank everyone at TSA, our interagency partners, and industry stakeholders — including airlines, airports, and solution providers — who provided input," he said.

On May 7, US Travel sent a letter to senators asserting among other things that the amendment would "significantly slow down checkpoint screening by making manual identity checks the default."

"This reduces the efficiency benefits for TSA PreCheck screening by requiring cumbersome processes, such as requiring all passengers to be offered a manual ID check first. According to an analysis of TSA data by U.S. Travel, Americans will wait an additional 120 million hours in TSA lines each year by significantly slowing down both PreCheck and standard screening lanes if this amendment is enacted," the group said.

The letter said the amendment would also "End the expansion of TSA PreCheck's Touchless Identity Solution, which would prevent most airports, airlines, and passengers from using the world-leading, opt-in security and facilitation service."

On the question of wait times, TSA spokesperson Alexa Lopez told *Inside AI Policy*, "We have been very clear that anyone may opt out of facial recognition technology without recourse or delay. At that point, the [Credential Authentication Technology] is used, but no camera. If we go back to manual ID checks, that could tap time on. Touchless ID with TSA PreCheck is particularly quick."

Asked to respond to the senators' letter, Lopez said, "TSA is using facial recognition technology in CAT-2 units at more than 80 airports across the country to improve transportation security effectiveness, efficiency, and the passenger experience."

TSA has said fraudulent IDs and imposters are an emerging threat to security and that the facial recognition technology represents a significant security enhancement because the facial recognition technology TSA uses helps ensure the person standing at the checkpoint is the same person pictured on the identification credentials.

But the senators note unacceptable error rates associated with the technology and said there is no side-by-side comparison of the system to manual checks performed by TSA workers, something Merkley's amendment would have addressed by requiring the Government Accountability Office to report such data to Congress.

"As of May 8, during this calendar year, fewer than one out of every one million passengers have complained to TSA about the facial recognition technology. At airport security checkpoints, few passengers are choosing to opt out illustrating there is a low volume of concern with TSA's use of facial recognition technology," Lopez said, reiterating that use of the technology is optional for travelers.

But Merkley has argued poor signage and fear of the consequences mean travelers would not be inclined to opt out of the face scans, and Pekoske has indicated an intention to eventually "require" the technology at all airports.

"This highlights a major issue with the 'opt out' approach to facial recognition," Seeley George said. "Whatever entity is administering this surveillance technology can say it's optional, until it isn't. This is why we so desperately need legislation protecting the public from this bait and switch."

House Judiciary panel examines use of AI to protect intellectual property

Posted May 10, 2024

A House Judiciary subcommittee held a hearing to examine the Biden administration's enforcement of intellectual property protections, where federal officials cited the role of artificial intelligence as both a hindrance and help in IP enforcement.

"AI-enabled IP theft is an emerging threat," Michael Ball, Department of Homeland Security acting assistant director of global investigations, said at a May 7 hearing by the Judiciary courts, intellectual property and the internet subcommittee.

Ball's comments about AI were echoed by other witnesses from the Justice Department and U.S. Customs and Border Protection, pushing back on suggestions by Republicans that the Biden administration was failing in its obligation to counter IP theft from China and other fraudsters.

Ball told lawmakers that DHS' IP Rights Coordination Center, which investigates fraud, "is using enhanced appropriations to further engage on AI, both in combating AI threats to IP and in leveraging AI to aid investigations."

He noted that President Biden's executive order for safe and secure AI "tasked the IPR Center to partner with private industry to identify emerging AI threats to IP and develop a training, analysis, and evaluation program to mitigate these threats."

And the center has "stood up a working group, comprised of subject matter experts from industry, government, and

academia," Ball said.

"This working group is also identifying new ways to leverage AI to aid in investigations," Ball told lawmakers.

"We utilize AI through" the DHS Homeland Security Investigations' Innovation Lab "which serves as HSI's physical and virtual hub for the development of new advanced analytics capabilities, tools, and enhanced processes," Ball said. "The HSI Innovation Lab utilizes AI to provide tools to agents and analysts to enhance capabilities and save time," he added.

At the same time, Deputy Assistant Attorney General Josh Goldfoot said the Justice Department is "looking at all the different ways that artificial intelligence changes the game in the enforcement of intellectual property laws."

"I think you can look at it from two different directions," said Goldfoot who leads DOJ's criminal division. "One is how does it make crime easier such as the situation you describe where people are using generative AI to create meritless trademark filings," he said in response to a lawmaker's question.

"Also, within the Department of Justice [we're] looking at how we can use it to improve our own enterprise and improve our ability to go after intellectual property crime," he told the subcommittee.

U.S. Customs and Border Protection's Brandon Lord told lawmakers that his agency is looking to use AI to improve its risk-assessment operations.

"As we pursue key regulatory updates and legislative changes, CBP continues to upgrade our facilities and provide our personnel with tools needed to efficiently process de minimis cargo," said Lord who leads CBP's trade policy and programs.

"We are installing state of the art scanning technology at our [ports of entry] and international mail facilities," he said, adding: "The agency is also advancing our investments in artificial intelligence and automated tools to assist personnel in risk-assessment."

Full committee ranking member Jerold Nadler (D-NY) cited a recent Government Accountability Office report calling for stronger trademark protections as a potential guide for federal enforcement officials.

The GAO report recommended the U.S. Trademark Office invest in fraud detection techniques in response to an anticipated increase in AI-generated fraudulent applications.

GAO said "academics told us that as generative AI becomes more specialized, filers could inundate the trademark review system with increasingly sophisticated fraudulent filings. These academics told us that the USPTO should get ahead of this issue and invest resources in prevention and detection to the fullest extent possible."

Nadler said federal authority for protecting IP "is clearly broad and wide ranging from enhancing cyber security and stopping copyright piracy to counterfeit enforcement and protection of trade secrets."

"And recent technological innovations have further complicated this already complex web of enforcement responsibilities," he argued.

He said the "widespread availability of 3D printing to create counterfeit goods" and the use of AI "to replicate copyrighted works" as well as advanced technology "to make pirated livestreams available to living rooms around the world, have all made it harder to protect Americans creative works."

Chairman Darrell Issa (R-CA) said the "purpose of today's hearing is to scrutinize the Biden administration's enforcement of existing intellectual property laws."

"IP is the foundation of our nation's economy, creativity and innovation, but annual losses due to lack of enforcement are costing the American economy nearly $1 trillion," he added.

Subcommittee ranking member Hank Johnson (D-GA) pushed back on the suggestion that the Biden administration is not doing enough to protect IP.

"The agencies represented today are staffed with dedicated and capable public servants, but the challenges they confront cannot be solved by the American government alone," Johnson said in his opening remarks.

"It is crucial that we work together with other governments and their law enforcement agencies to combat the real dangers of IP theft to the health of our economy and the safety of our citizens," he said.

Information software group says federal procurement policies meet needs related to AI

Posted May 10, 2024

The Software and Information Industry Association says the federal government should rely on existing rules and frameworks as it considers ways to ensure "responsible procurement" of artificial intelligence products and services under an Office of Management and Budget memo on implementing President Biden's Oct. 30 AI executive order.

"We believe the administration should continue encouraging the adoption of risk-based AI governance practices in general, as this approach is crucial in understanding AI use cases across the government. We believe it is also important to recognize that the desired goals of the OMB AI memo can be achieved without reshaping the scope of the government procurement process," SIIA says in comments to OMB.

OMB on March 28 finalized guidance for federal agencies on implementation of the AI executive order and the following day published a request for information on how it should apply the EO's provisions on responsible federal

procurement of the technology. The 30-day comment period on the RFI closed on April 29.

Industry groups including the Information Technology Industry Council, BSA-The Software Alliance and the U.S. Chamber of Commerce urged OMB to rely on "commercial solutions" and argued that vendor safety assessments can meet the federal government's needs.

SIIA says in its comments, "Existing processes for government procurement of information technologies will continue to be effective. Standards and frameworks such as the NIST AI Risk Management Framework and ISO standards should serve as a starting point when considering responsible AI procurement. We believe that reliance on these existing frameworks and standards will largely apply in the context of AI technologies."

SIIA describes itself as "the principal trade association for companies in the business of information. Our members include roughly 375 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services."

The group expresses support for federal efforts "to advance proactive AI policy efforts. Our association represents companies that develop and deploy these engines, as well as those who create the information that feeds environments. SIIA is uniquely positioned to provide insight on policies to encourage the federal government's responsible adoption of AI, as well as procedures designed to advance a risk-based approach to AI-related risks and opportunities."

Addressing the particulars of AI procurement policy, SIIA emphasizes the need to "delineate" responsibilities between vendors and agencies.

"Vendor and government agencies each have unique positions within the procurement ecosystem. We believe that vendors are best positioned to provide information about their AI services. In parallel, government agencies who are familiar with the intended application of the technologies are best positioned to ensure proper deployment and risk assessments," SIIA says.

"This delineation between vendors and agencies will allow for the most efficient use of resources on both ends. This is particularly the case in the context of AI being used in high-risk ways, as the developer of high-risk AI systems should be able to provide documentation as to how risks are being identified and mitigated. This is already being facilitated by our member companies that provides AI service cards, which explain the use case for which the service is intended, how machine learning is used by the service, and important considerations for responsible use."

"With this type of transparent documentation," SIIA says, "agencies are equipped to make informed decisions when deploying systems in a responsible manner in relation to a given use case."

On risk mitigation, the group says, "We believe the OMB can encourage agencies to take effective steps to mitigate the risk of AI tools producing harmful or illegal content and promoting equitable outcomes by leveraging existing best practices and standards. In doing so, agencies can prioritize procuring products that align with OMB's M-24-10 guidance on responsible and safe AI deployment."

It says, "Since no two agency use cases are the same, we encourage agencies to continue their engagement with a diverse set of stakeholder groups who are facilitating discussions on what would best resemble these desired principles."

Further, SIIA says, "Government agencies have the ability to evaluate products that would be the best fit by engaging with vendors during the market research. This can include requesting demos, surveying and comparing options in the marketplace. OMB can encourage agencies to incorporate equity considerations into their due-diligence process as they identify the technologies it needs and the most appropriate method for procuring, deploying, and monitoring them post-award."

Klobuchar prepares to mark up landmark legislation on protecting elections from AI

Posted May 9, 2024

The Senate Rules Committee is scheduled on May 15 to mark up legislation requiring the disclosure of artificial intelligence used by political campaigns and banning deceptive AI-generated content to protect the upcoming election from the threat of disinformation.

The committee action comes as Chair Amy Klobuchar (D-MN) has been calling on her colleagues for weeks to help build bipartisan support for the landmark legislative proposals.

The committee's "business meeting" next week will include consideration of S.2770, to prohibit the distribution of "materially deceptive AI-generated audio or visual media relating to candidates for federal office," and S.3875, to amend the Federal Election Campaign Act of 1971 to provide transparency for the use of content that is "substantially generated" by AI in political ads by "requiring such advertisements to include a statement within the contents of the advertisements if generative AI was used to generate any image, audio, or video footage in the advertisements," says a committee announcement of the markup.

Also, senators will consider S.3897, "to require the Election Assistance Commission to develop voluntary guidelines for the administration of elections that address the use and risks of artificial intelligence technologies,"

according to the committee.

Klobuchar announced her intentions to mark up the legislation at an April 16 hearing by the Judiciary subcommittee on privacy, where senators renewed their calls for the leaders of both parties to schedule floor votes on multiple bipartisan proposals intended to protect the nation's democratic institutions from an alarming increase in the use of AI-generated deepfakes to sow civil unrest.

"We cannot wait. We are scheduling a markup of our bill. And we are going to have to work" to gain bipartisan support, Klobuchar said at the hearing without offering a specific date for the markup.

Klobuchar introduced S.2770 in September with Sens. Josh Hawley (R-MO), Chris Coons (D-DE) and Susan Collins (R-ME).

At the hearing, Klobuchar asked Hawley for "help, and others on our bill" including Coons and Collins "to get the votes, not just to, you know, we can obviously pass it, but I'd like to get a really strong vote coming out of committee," referring to the upcoming Rules markup.

Hawley renewed his call for congressional action to avoid what he described as a "painfully apparent" imminent catastrophe for U.S. democratic institutions.

"But now it's really time to vote. And I just call on the leadership of both parties in the Senate, both parties, the leadership needs to support an effort to get a vote," Hawley said at the subcommittee hearing.

Hawley is the ranking member of the Judiciary privacy subcommittee and Coons chairs the intellectual property subcommittee, but neither of them are members of the Rules Committee. Collins is the ranking member of the Appropriations Committee.

Senate Majority Leader Charles Schumer (D-NY) and Minority Leader Mitch McConnell (R-KY) are members of the Rules Committee, so bipartisan approval could provide the bill strong momentum for a floor vote.

The bill, the Protect Elections from Deceptive AI Act, would prohibit the distribution of deceptive AI-generated audio, images or video related to federal candidates in political ads and certain issue ads "to influence a federal election or fundraise," according to a summary.

The bill would allow affected candidates to seek damages in court, and contains an exemption for satire and news that is "consistent with First Amendment" free speech protections, the summary says.

The Rules Committee held a hearing on the bill where ranking member Deb Fisher (R-NE) raised concerns about the free-speech implications of banning certain types of content in political advertising.

Klobuchar introduced S. 3875, AI Transparency In Elections Act, on March 7 with Sen. Lisa Murkowski (R-AK). S. 3897, Preparing Election Administrators for AI Act, was introduced by Klobuchar on March 11.

Tech industry group tells OMB to follow the EU's lead in crafting procurement language for AI

Posted May 9, 2024

The Office of Management and Budget should look to the European Union for an example in developing provisions agencies can insert into contracts for responsibly purchasing artificial intelligence goods and services, according to the Center for Data Innovation.

"OMB should support the creation of standard clauses that align with the requirements in the AI M-memo just as the EU is doing for the requirements of its AI Act," the tech group said in April 29 comments referencing OMB's March 28 memo, which agencies are required to follow in implementing President Biden's Oct. 30 executive order on AI.

CDI is an initiative of the Information Technology and Innovation Foundation, which is funded by tech-industry giants and other major U.S. corporations. Its comments reflect an eagerness to participate in the particulars of AI acquisition that is shared by civil society groups as debate about the technology's implications for minorities continues to hold the public's attention.

"The EU government is supporting external experts in peer reviewing the draft clauses through public workshops and requests for comments and OMB should follow suit for any standard clauses it creates," CDI wrote.

The group highlights OMB's instruction noting agencies must "follow a set of minimum practices when using safety-impacting AI and rights-impacting AI, or else stop using AI in their operations."

"To ensure that federal contracts for the acquisition of an AI system or service align with the guidance in this memorandum, OMB should support the development of voluntary standard terms for AI contracts to make procurement more efficient and expand access to federal contracts to as diverse and large a pool of vendors as possible so federal agencies can access the best systems," the comments read.

CDI provided an example of what it said should be on a menu of clauses contracting officials can select from when seeking AI goods and services, adding the U.S. "should build on [the EU's] work for an American variant of these common clauses that aligns with the AI M-memo."

Quoting from a May 2023 roundtable on AI procurement, the group said "one proposed clause public organiza-

tions could use is: 'The Supplier ensures that the Data Sets used in the development of the AI System are relevant, representative, free of errors and complete. The Supplier ensures that Data Sets have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the AI System is intended to be used. These characteristics of the Data Sets may be met at the level of individual data sets or a combination thereof.'"

"This clause is to help organizations ensure the systems they get from vendors would align with Article 10 of the approved EU AI Act, which states a high-risk AI system must have training, validation and testing data sets that are relevant, representative, free of errors, and complete," CDI wrote.

However, the comments also highlight the lack of congressional action on AI in the U.S. and call into question the basis of the wholesale requirements in the OMB memo.

"But the United States has not passed similar legislation with these requirements, and in many cases, providing error-free or complete data is not feasible, practical, or necessary," the group said.

Witness at Senate hearing praises 'permissible purposes' in draft privacy bill, urges AI for cyber defense

Posted May 9, 2024

Witnesses testifying before a Senate Commerce subcommittee cited artificial intelligence as a reason for lawmakers to both pass legislation featuring strong data minimization provisions and to temper their approach to allow for cybersecurity.

"We leverage AI across our systems and capabilities, and we are able to detect 2.3 million unique attacks that weren't there the day before. This is a process of continuous discovery, and we're able to leverage our security data and those AI tools to block 11.3 billion attacks per day," said Sam Kaplan, senior director of public policy and government affairs for Palo Alto Networks, adding "that's just one player, one company in the cyber ecosystem."

Kaplan was a witness — along with James Lee, COO of the Identity Theft Resource Center, Prem Trivedi, policy director of the New America think tank's Open Technology Institute, and Jake Parker, senior director of government relations for the Security Industry Association — at the May 8 hearing of the Senate Commerce subcommittee on consumer protection, product safety and data security.

He cited the cybersecurity firm's use of AI in highlighting a significant exception for data covered in a draft privacy compromise — the American Privacy Rights Act — which supporters say will form a foundation for regulating artificial intelligence, with adversaries like China leveraging American's data to build their own systems providing additional urgency.

The APRA draft was released in April by Senate Commerce Chair Maria Cantwell (D-WA) and House Energy and Commerce Chair Cathy McMorris Rodgers (R-WA). The legislation has yet to be formally introduced or scheduled for markup.

"To stay ahead of this evolving threat landscape, cybersecurity professionals regularly leverage security data, which is the network telemetry, the one isn't the zeros, the malware analysis, the IP addresses the vulnerability enumeration that we must ingest and analyze in real time to optimize cyber defenses," Kaplan said in his opening statement. "To that end, we are heartened to see cybersecurity generally included in privacy frameworks, as a permitted purpose that companies like ours can use to collect, process retain and transfer security data, to in turn better protect those systems and data from compromise."

Kaplan also took the opportunity to build on comments that Lee, from the Identity Theft Resource Center, made after describing data minimization provisions as crucial to the privacy legislation.

"My watch out on the Privacy Rights Act would be: be aware of the law of unintended consequences," he said. "We talked about … data minimization, we still need data and we need it for some very specific purposes because it's used for anti-fraud, it's used for identity verification, to prevent identity crimes. So in our zeal to protect consumers and give them access, we also have to be realistic that we still need some data."

Kaplan quickly followed that, noting, "One of the beneficial aspects of the APRA that we see is those strong, permissible purposes for cybersecurity companies. Mr. Lee also talked about the uses of data, both for our cyber defenses but also in artificial intelligence."

"The utility of this data, I think, is proven and that's where sort of the flexibility of something like the permissible purposes in the APRA are critical to securing everybody's data," Kaplan said.

Citing EU rules

Among the more controversial aspects of the European Union's General Data Protection Regulation was the classification of IP addresses as covered sensitive data.

Subcommittee ranking member Marsha Blackburn (R-TN) criticized the GDPR as going too far, but cited China's AI ambitions in asking how lawmakers can build on legislation such as their recent success in passing a ban on TikTok

while it is owned by a China-controlled entity.

"The data security threat from China is broader than just TikTok and a more holistic approach, rather than playing whack a mole, is required as this problem goes beyond apps," she said.

More broadly, in her opening statement, Blackburn said: "In our daily lives here in the U.S. consumers have valid questions about how their data is going to be used to train these large language models and AI applications. I hope today that we will discuss why we need federal privacy and security legislation to combat these threats."

MITRE announces 'sandbox' enabling federal agencies to test AI systems

Posted May 9, 2024

MITRE Corporation expects to have operational by the end of the year a "sandbox" allowing federal agencies to test artificial intelligence systems in response to President Biden's executive order for safe and secure AI technologies.

The new testing program announced May 7 will be powered by MITRE's recent purchase of NVIDIA's supercomputer system DGX SuperPOD, with federal agencies able to access the system under existing contracts with any of the six federally funded research and development centers operated by MITRE.

"MITRE will apply the Federal AI Sandbox to its work for federal agencies in areas including national security, healthcare, transportation, and climate," the nonprofit think tank says in a statement announcing the new testing program.

"Our new Federal AI Sandbox will help level the playing field, making the high-quality compute power needed to train and test custom AI solutions available to any agency," said MITRE senior vice president and chief technology officer Charles Clancy in the statement.

MITRE says the testing and development program was initiated in response to Biden's Oct. 30 executive order which encourages federal agencies to adopt AI systems to improve government operations, among other measures. The research group says its new testing program will provide agencies with the capacity to evaluate AI systems to ensure they meet their policy goals and requirements.

"Today, few federal agencies have adequate access to large-scale computing infrastructure. This situation inhibits public sector innovation by limiting the creation and evaluation of customized AI tools like large language models (LLMs) similar to ChatGPT," MITRE says.

It's new "flagship AI supercomputer" will "streamline and expand" the government's access to "the high-end computing that drives modern AI," MITRE says.

"Sandbox capabilities offer computing power to train cutting edge AI applications for government use including large language models (LLMs) and other generative AI tools," according to the statement.

"It can also be used to train multimodal perception systems that can understand and process information from multiple types of data at once such as images, audio, text, radar, and environmental or medical sensors, and reinforcement learning decision aids that learn by trial and error to help humans make better decisions."

The NVIDIA supercomputer system powering the experimentation initiative "is capable of an exaFLOP of 8-bit AI compute, meaning it performs a quintillion math operations each second to train and deploy custom LLMs and other AI solutions at scale," according to MITRE.

"An AI supercomputer at this scale is ideal for training new, government-specific large frontier AI models, including LLMs, other generative AI, machine vision and multimodal perception systems, and reinforcement learning decision aids," the statement says.

MITRE's announcement comes weeks after Sen. Mark Warner (D-VA) gave a speech at a MITRE-hosted event where he unveiled plans for legislation to codify the AI safety standards that are being developed under Biden's order.

Warner said he's working on a bipartisan basis to draft legislation that would take the standards being developed by the National Institute of Standards and Technology for use by federal agencies and codify them through federal law.

Warner also highlighted the role of the MITRE labs to help the U.S. reassert global leadership on the development of and standards for AI technologies.

Along those lines, MITRE has joined the NIST AI Safety Institute consortium to assist with research on testing the safety of AI systems under Biden's order.

"MITRE has submitted a letter of interest to the safety institute to be part of the consortium," Michael Garris, a senior technical advisor at MITRE's AI and Autonomy Innovation Center, told *Inside AI Policy*.

Garris was attending a March 25 ribbon-cutting ceremony for MITRE's AI Assurance and Discovery Lab at its headquarters in McLean, VA, along with Sen. Warner and Reps. Gerry Connolly (D-VA) and Don Beyer (D-VA). NIST AI Safety Institute Director Elizabeth Kelly was also in attendance at the MITRE event.

Data concerns prompt senator's call to ban connected cars from China

Posted May 9, 2024

Senate Banking Chairman Sherrod Brown (D-OH) wants the Biden administration to issue a rulemaking banning the import of Chinese-made connected vehicles that could transmit sensitive data back to China and pose both cybersecurity and artificial intelligence-related national security risks.

"Given the access and information that connected vehicles have regarding both Americans' sensitive personal data and U.S. infrastructure, I encourage you to issue a notice of proposed rulemaking that includes prohibitions on finished vehicles and technology that is designed, developed, manufactured, or supplied from the People's Republic of China (PRC)," Brown said in an Apil 30 letter to Elizabeth Cannon, executive director of Commerce's Office of Information and Communications Technology and Services.

"Given China's civil-military fusion, it is inevitable that both finished vehicles and technology would enable the Chinese Communist Party to access sensitive personal data of Americans and of critical U.S. infrastructure," the senator wrote.

This is the latest salvo in Brown's campaign to counter technological advances by China that could threaten U.S. national and economic security. The Chinese government's collection of data on U.S. citizens and entities has long concerned security pros over its potential use in the development of AI models as well as possible weaponization.

Brown in January held a hearing on "outpacing China in emerging technology," where witnesses called for expanding restrictions on investments in China to block Beijing's efforts to develop artificial intelligence technologies. "Today we will discuss how we should rethink and reorient how economic security programs are implemented to address the full range of risks posed by China," Brown said at that hearing.

Brown's office said in a May 8 release, "Connected vehicles — both those with internal combustion engines and electric vehicles — collect, transmit, and store a range of sensitive information, including biometric data like fingerprints and voice recordings, vehicle location, sensor data and images, financial information, and vehicle information."

The release said, "Chinese-made cars and the underlying technology enable the Chinese Communist Party to access sensitive personal data of Americans and of critical U.S. infrastructure, presenting unacceptable national security risks."

Commerce's Bureau of Industry and Security issued an advance notice of proposed rulemaking on March 1 with an April 30 comment deadline.

It was issued under the authority of a 2019 executive order on "Securing the Information and Communications Technology and Services Supply Chain." The ANPRM "recognizes the benefits of CV technologies and does not imply through this ANPRM that technologies such as vehicle-to-everything (V2X) communications are generally unsafe for use in the United States," Commerce says in the March notice.

It says the proposal is "narrowly focused" on foreign adversaries.

Now, Brown is pushing to make the ANPRM a final rulemaking. The senator "is calling on the Administration to act before Chinese-manufactured connected vehicles become widespread in the United States, and submitted this public comment letter to the Department of Commerce as they work to finalize rules regarding connected vehicles," according to the release.

Amid the benefits of connected vehicles, Brown wrote, "this same technology and information also presents national security risks — whether they be backdoors that could allow vehicles to be accessed remotely or disabled or information or data that could be exploited to harm American families. Certain connected vehicles plug into electrical charging stations that could be targeted by malicious actors to affect vehicle performance or electrical grid infrastructure."

Brown said, "This rulemaking is an important opportunity for the Office of Information and Communications Technology and Services to establish rules that recognize and address the national security threats posed by advanced Chinese technology and access to sensitive data."

He called on Commerce officials "to carefully consider public comments provided during this ANRPM comment period and to move with deliberate speed to the next stage of this rulemaking process by issuing a NPRM."

Court tells OpenAI to investigate board discussions on ChatGPT training in copyright lawsuit

Posted May 8, 2024

OpenAI has been ordered by a federal district court to investigate whether current and former board members and employees discussed on social media the training of its generative artificial intelligence model, ChatGPT, in response to a request by class-action plaintiffs who accuse the company of copyright infringement.

"The court finds that the burden associated with undertaking this inquiry is minimal and that it is proportionate and responsive to the needs of the case," says a May 7 order by U.S. district court for northern California Magistrate Judge Robert Illman in *Tremblay et al. v. OpenAI et al*.

"If all current directors and employees report that they have engaged in no such discussions on their social media accounts, Defendants are ORDERED to certify that fact to Plaintiffs, which will put the matter to rest," the order says.

"If, on the other hand, any current director or employee answers that inquiry in the affirmative, Defendants are

ORDERED to gather and disclose that person's relevant social media username(s) forthwith," it adds.

The order closes the door, for now, on a simmering dispute in the case over access by plaintiffs to information about the training of ChatGPT that they say will prove their allegations that the company violated their copyright protections.

"In essence, Plaintiffs contend that because a large language model's output is reliant on the material in its training dataset, '[e]very time it assembles a text output [in response to user queries], the model relies on the information it extracted from its training dataset,' which results in ChatGPT sometimes generating summaries of Plaintiffs' copyrighted works and benefiting commercially from the use of Plaintiffs' and Class members' copyrighted works," the order says.

Plaintiffs are seeking "basic information" on the social-media usernames of OpenAI employees who may have used those accounts to communicate "on the subjects of the litigation," according to their request.

"Plaintiffs explain that Defendants' directors and personnel may operate some of their personal social media accounts pseudonymously, making it difficult or impossible for Plaintiffs to uncover discussions relevant to this action having taken place through such accounts by other means," according to the order.

To argue for this information, plaintiffs cited an example of Elon Musk, a co-founder and early investor in OpenAI, stating "in a recent deposition in a separate action" that he uses pseudonymous social-media accounts.

Defendants, however, argued that the request was too far reaching and that the company does not have access to the social-media accounts of its employees.

"In essence, Defendants state that they do not have the requested information in their 'possession or custody' because 'the company does not systematically collect from its employees and Board members information about personal social media accounts, or monitor those accounts in the ordinary course of business,'" the order notes.

Yet Magistrate Illman wrote: "As to past employees, Defendants are ORDERED to produce the social media usernames of any such persons if Defendants know, or learn, that any that such persons have engaged in discussions on social media that might be relevant to claims or defenses in this case, and the social media username(s) of such persons are known to Defendants."

The court did reject a request by plaintiffs for information about individuals and entities that have at least a five percent ownership interest in OpenAI on the assumption that they "may have sought to exert influence and/or voice concern vis-à-vis decisions by Defendants," according to the order.

"Plaintiffs' portion of the letter brief does not indicate any concrete basis on which the court could conclude that entities or persons owning more than 5% of the shares of OpenAI actually would have (rather than could have) any relevant documents or information, or that they actually (rather than might have) sought to exert influence or voice concerns about OpenAI's relevant business decisions," the order says.

"The asserted basis for compelling this discovery appears to be purely speculative — as does the contention that the identities of these shareholders would help Plaintiffs 'understand the Defendants' corporate relationship and structure of relationship,'" the order adds in rejecting the plaintiffs' request.

The court in February partially granted a motion for dismissal by OpenAI, telling plaintiffs to narrow their complaint.

Nowhere in their complaint do plaintiffs "allege that Defendants reproduced and distributed copies of their books. Accordingly, any injury is speculative, and the unlawful prong of the [California Unfair Competition Law] claim fails for this additional reason," the court ruled earlier this year.

Also, "Plaintiffs here have not alleged that ChatGPT reproduces Plaintiffs copyrighted works without" copyright management information under the Digital Millennium Copyright Act," the court ruled in granting partial dismissal and allowing plaintiffs to narrow their complaint which was due in March.

NAIRR projects include use of AI to improve image recognition, detect deepfakes

Posted May 8, 2024

Among the first batch of projects to be supported by the recently established National AI Research Resource pilot program is a proposal to use generative artificial intelligence to improve image recognition for the purpose of "discriminative" tasks, according to a summary to project.

"We will develop unsupervised unified representations, for generative and discriminative tasks, to be used as general-purpose representations for various downstream tasks like image recognition, reconstruction, and synthesis," says an abstract of a research project approved for NAIRR support as unveiled at a May 6 White House event.

"Such unified models can be efficiently finetuned for multiple downstream tasks, as opposed to having to pre-train large, expensive models separately for different tasks," the summary says.

The project, titled "Unified Representation Learning," has been allocated 100,000 node hours of computation support by the Department of Energy's Oak Ridge National Laboratory.

Another project will use algorithms to enhance the detection of AI-generated deepfakes which is a growing concern among those seeking to protect the upcoming election from deceptive AI-generated content.

The projects, along with 33 others, were announced by White House Office of Science and Technology Policy

Director Arati Prabhakar and National Science Foundation Director Sethuraman Panchanathan, and offer a first look at how the AI research network hub will be used to further the Biden administration's goal of developing safe and secure uses of the technology.

The NAIRR was announced as a pilot program by the NSF in January under President Biden's Oct. 30 executive order on AI. The research hub is intended to broaden access to the resources for developing AI technologies beyond big tech firms by offering access to the computation capacities of government labs and participating universities and private companies.

The research program has broad industry support and bipartisan backing in Congress with the Senate Commerce Committee poised to mark up legislation that would provide full funding and authorization for the NAIRR program.

And the scope and intentions of the initial projects being supported by the NAIRR could foreshadow the program's trajectory and continued support for it.

Of the 35 announced projects, four are categorized as AI systems and computer science and include research on building "reliable and secure AI surrogates for large-scale" scientific simulations and developing "a benchmark hydrologic dataset" for "assessing climate impacts on mountainous hillslopes," according to the summaries.

Other project categories include "Educational Sciences", "Health Sciences", "Biochemistry and Molecular Biology Clinical Medicine" and "Agriculture, Forestry, and Fisheries".

A project for developing "safe autonomous systems" seeks to do so by "aligning [those systems] with human preferences," according to the summaries.

"In this work, we study the problem of learning robot policies and reward functions that are aligned with societal scale objectives and human preferences," says the project abstract.

"This ensures the robot policies learned satisfy desirable safety specifications and can robustly act and interact in human spaces. We plan to leverage and refine large vision-language models that can act as proxy preferences of humans via human feedback. Specifically, we will pretrain and adapt robot policies initialized with these VLMs to achieve the alignment objective," the abstract says.

Another project will examine the detection of AI-generated deepfakes, which is a hot-button issue on Capitol Hill amid efforts to protect the upcoming election.

"DeepFake, a term increasingly mentioned in the news and social media, refers to highly realistic fake images, audios, and videos created using AI algorithms," according to the project summary.

"By creating illusions of an individual's activities that did not occur in reality, DeepFakes can cause serious harm when they are weaponized."

The project's sponsors are proposing a "proactive strategy" with a "novel framework" for detecting deepfakes "that evade current forgery-specified detectors."

"The framework aims to find common features in various forgeries, promoting learning in a model on a flattened loss landscape to improve the detector's ability to generalize," the project abstract says.

"All algorithms developed throughout this project will be made openly accessible as open-source software on GitHub," it adds.

At the White House event announcing the NAIRR projects, both Prabhakar and Panchanathan called for congressional action to authorize the research program, arguing that bringing to scale all of the proposed projects will require additional funding.

"But remember the word pilot, which means that it calls for a full-scale implementation rather soon," said Panchanathan about the need for congressional authorization of the NAIRR program.

"And for that full scale implementation, I'm grateful to Congress, for working on this in a bipartisan manner, both in the House and the Senate side, to be able to have the AI caucuses advance this idea of how do we get more resources," he said, adding "I'm very excited by that."

TSA expansion of facial recognition tech target of bipartisan FAA amendment

Posted May 8, 2024

Privacy advocates are echoing calls from a new bipartisan group of senators in urging leaders of the upper chamber to support an amendment to the Federal Aviation Administration reauthorization bill that would halt the Transportation Security Administration's rollout of facial recognition technology at airports across the country.

The amendment, introduced by Sen. Jeff Merkley (D-OR) with support from Sens. John Kennedy (R-LA) and Roger Marshall (R-KS), is one of almost 200 that lawmakers are trying to attach to the bill, which is considered "must pass" before May 10 when the current congressional authorization expires.

Senate leaders have both supported a robust amendment process and discouraged bogging the legislation down with provisions that may or may not be germane amid limited opportunity to get congressional action across the finish line.

"While there is uncertainty about whether some of the many amendments submitted for the FAA reauthorization will make it through, we believe that since this amendment directly relates to federal aviation policy it should be

included," Fight for the Future campaigns director Caitlin Seeley George said in a May 6 press release.

The group's release flagged a May 6 letter of support for the amendment signed by a host of civil society groups, including the Algorithmic Justice League, the ACLU, Public Citizen, the Project on Government Oversight, Demand Progress the Center on Race, Inequality, & the Law at NYU School of Law, the Electronic Frontier Foundation and the Electronic Privacy Information Center.

It also highlighted a May 2 letter to Senate leadership signed by seven Democrats, six Republicans and independent Sen. Bernie Sanders (VT).

Use of Facial Recognition has grown at TSA and other Department of Homeland Security agencies with department officials citing National Institute of Standards and Technology testing that they say reflects a high degree of accuracy. But civil society advocates have stressed a need for "real-world" data on the performance of the technology which is associated with higher rates of error for minorities.

"This is a very reasonable step to slow the rollout of this highly controversial tech and require the TSA to report on its current use and share data on misidentification rates, among other things," Seeley George said in the press release.

TSA Administrator David Pekoske has reportedly refused to share information from TSA's years-long facial recognition technology pilot with senators calling for a pause on plans to expand its use to hundreds of airports across the country. And while DHS officials have highlighted use of the technology is optional for travelers, the advocates note that isn't easily apparent.

"We call on Congress to use this opportunity to freeze the expansion of facial recognition in airports to protect travelers so that Congress can conduct meaningful oversight of the program," the groups wrote. "If the TSA is focused on expansion rather than remedying existing issues, it will fail to fully address these concerns."

The senators' letter, which noted Pekoske's indication of plans to eventually require across-the-board use of facial recognition technology, also expressed dissatisfaction with error rates reported by TSA while the agency asserts benefits to security and efficiency.

"In response to Congressional inquiries, TSA has not produced evidence that more false identification documents have been discovered since their implementation of facial recognition," the senators wrote. "The 3 % error rate cited by TSA represents more than 68,000 mismatches daily if used on all 2.3 million daily travelers."

As related business interests have pushed for greater use of facial recognition technology, text of the giant FAA reauthorization bill now includes a provision for the head of the agency to report to Congress on lessons learned, including potentially from China, on use of the tech for improving airport safety and efficiency.

The senators' letter cautioned against the spread of facial recognition tech to other areas if it is not stopped in the aviation bill.

"The potential for misuse of this technology extends far beyond airport security checkpoints," they wrote. Once Americans become accustomed to government facial recognition scans, it will be that much easier for the government to scan citizens' faces everywhere, from entry into government buildings, to passive surveillance on public property like parks, schools and sidewalks."

They said: "The FAA re-authorization bill is a key opportunity to provide needed oversight of TSA's facial recognition program. Should Congress delay, TSA's facial recognition infrastructure will soon be in place at hundreds of cities across the America and it will be that much more difficult to rein in facial recognition surveillance by the government."

House approves bipartisan bill limiting AI-generated comments on draft federal rules

Posted May 8, 2024

The House approved by voice vote a bipartisan bill requiring federal agencies to identify and set aside artificial intelligence-generated comments on proposed rules, with the intention of weeding out automated duplicates that advocacy groups might use to overwhelm and influence regulatory policymakers.

"The term 'computer-generated comment' means a comment the substance of which is primarily generated by computer software, including through the use of artificial intelligence, rather than by a human being," says the bill, H.R. 7528, in identifying the comments to be singled out as duplicates for removal from federal agencies' regulatory dockets.

The House on May 6 approved by voice vote H.R. 7528, the Comment Integrity and Management Act, marking a significant step by the federal government to establish definitions and set controls on the use of AI in the rulemaking process. The bill amends the E-Government Act of 2002.

The bill requires the White House Office of Management and Budget to issue guidance to federal agencies within eight months on identifying and removing duplicate AI-generated comments submitted on proposed rules. The heads of federal agencies are required within one year to issue policies "with respect to the posting and consideration of computer-generated comments and mass-comments during the rulemaking process," in compliance with the OMB guidance.

The legislation, however, states the intention of lawmakers to avoid interfering with the notice-and-comment

process central to federal rulemaking.

"Nothing in this Act, or any amendment made by this Act, shall be construed to minimize an agency's due consideration of mass comments submitted during the rulemaking process," the bill text says.

Agency heads, "instead of making available through the electronic docket of the agency each mass comment accepted by electronic means under subsection 19 (c), may: (i) make available through such docket only a single representative sample of each such mass comment; and (ii) in the case where mass comments take the form of variations on certain standardized but not identical language the agency may make available through such docket a single copy of one of the variations of the mass comment," the bill says.

The bill also requires the Government Accountability Office and the Comptroller General to report back within two years to the House oversight and Senate governmental affairs committees on the effect that the restrictions for AI-generated comments has had on the federal rulemaking process.

The bill is based on recommendations by the Administrative Conference of the United Sates on identifying "computer-generated and falsely attributed comments."

"Agencies should manage mass comments by using tools that allow them to de-duplicate comments, encouraging the inclusion of multiple signatures on a single comment, and considering various ways to display comments, such as posting a single representative sample of nearly identical comments received," says the June 2021 recommendations by the ACUS, an independent agency established by Congress in 1964 to promote government efficiencies.

"Agencies should manage computer-generated comments by flagging comments they have identified as computer-generated, displaying and storing them separately from other comments, and using reCAPTCHA or similar tools to ensure comments are submitted by humans," the agency also recommended.

The House Oversight and Accountability Committee approved the bill as a substitute amendment on March 7 by a 31-9 vote. There is no companion bill in the Senate.

OpenAI's Altman sees progress on election security and other AI policy challenges

Posted May 8, 2024

OpenAI CEO Sam Altman said election security efforts related to artificial intelligence challenges have gone better than expected this year, while expressing confidence in his company's approach to developing the groundbreaking technology and how it aligns with an emerging policy landscape, during a May 7 Brookings Institution event.

"We haven't seen the predicted wave of AI-generated disinformation yet, though we could," Altman said. "We've built up the technical defenses and the societal antibodies" to AI-generated and distributed disinformation targeting elections in the United States and around the world this year, he said, noting that he remains concerned about "very targeted, customized" disinformation campaigns.

"I will be paranoid until Election Day and beyond," he said, "but I'm very happy to see this level of collaboration."

Altman said "one challenge has been everyone is cautious about antitrust standards, but the people involved really care about this."

"I feel reasonably good about our ability to respond" to a variety of security and safety challenges, Altman said in a wide-ranging discussion hosted by the Strobe Talbott Center for Security, Strategy, and Technology at Brookings. Michael O'Hanlon and Valerie Wirtschafter moderated the session.

Altman was named last month to the new Artificial Intelligence Safety and Security Board launched by the Department of Homeland Security under President Biden's October executive order on AI. The board held its first meeting on May 6 and had "a robust discussion" on how AI can be "harnessed to advance cybersecurity," Homeland Security Secretary Alejandro Mayorkas said in a May 7 speech at the RSA Security conference.

OpenAI shook up both the tech sector and the government policy world in November 2022 with the release of the generative AI-powered ChatGPT chatbot.

Altman noted there was more concern and discussion of AI's potential sociological impacts a year ago with the launch of GPT-4, but as the conversation about apocalyptic outcomes receded, so did that conversation.

"The speed and magnitude of the sociological impact still needs discussing," he stressed. "We need to continue having this discussion."

He said an "all of society" engagement is needed to address potential risks, drawing in developers, application providers, civil society and government.

But Altman said OpenAI's "iterative process" for development "has generally worked well for us," describing an approach that has involved release of AI products for review by "a few thousand" and then a "few million" people with extensive interactions.

Under that process, he said, OpenAI has added external red-teaming, auditing, "and will add government testing" to the assessments of the company's AI tools.

He said "compute" capacity is "the most valuable asset" in the development of AI, adding "we need to build as

much as possible … I would like to see this located in the United States."

The private sector will lead in investment in "compute," he said, but government investment will be needed as well.

"I feel good about the manufacturing of chips [in the U.S.], we're getting there," he said. But he acknowledged the huge energy demands of running data centers remains a challenge.

Altman also raised questions about the way President Biden's executive order uses compute power to assign greater safety responsibilities to the most powerful AI models. "I appreciate the spirit of setting a numeric value," he said, observing that the large tech firms developing the most powerful models "can handle the most regulatory overhead."

But he said smaller AI models are becoming increasingly powerful as well and called for more widely applicable safety tests.

In wrapping up, Altman said AI "should be a top-of-mind issue" for American voters, who should want to ensure that future policies support U.S. leadership in the development and deployment of AI.
