INSIDE AI POLICY

Exclusive news on the burgeoning debate over regulating artificial intelligence

Vol. 2, No. 19 — May 7, 2024

Sen. Rounds says ‘next Congress’ for passage of major AI legislation

Posted April 30, 2024

Sen. Mike Rounds (R-SD), a leading voice on Senate efforts to set guardrails on the use of artificial intelligence, says “next Congress” is a likely timeline for seeing movement on major AI legislation, while noting that any bill that comes out of his chamber will still have to pass the fractious House.

“It could be next Congress, but I think you’re going to see proposed legislation this Congress,” Rounds said today at a Punchbowl News event on AI impacts.

“Now, something getting passed Congress, … it’s got to be House and Senate, but you got to start someplace,” he said, adding, “The House is working on it now, as well.”

He said, “The fact that we’re talking about it, bringing it in, is a step in the right direction.”

Rounds’ comments are the latest indication of a timeline for Senate action on AI legislation, suggesting a slower schedule than indicated last year after the conclusion of a series of closed-door “insight” forums hosted by Rounds and others under the direction of Senate Majority Leader Charles Schumer (D-NY).

At the Punchbowl event, Rounds stressed a cautious approach to legislating on AI to avoid “doing damage” while promoting the development of the technology in the United States.

“We don’t want to do damage. We don’t want to have a regulatory impact that slows down our development, allows development [of AI] near our adversaries to move more quickly,” he said.

“But at the same time, we want to provide incentives so that development of AI occurs in our country, rather than other places around the world,” he added.

Yet he left open the door for some AI-related legislation this year by the various committees, saying the forums hosted last year with industry leaders and other AI policy stakeholders were intended to “educate” committee leaders and their staff “to incorporate the need to recognize AI’s impact on the areas where they were already creating laws.”

He also endorsed the use of open-source datasets while acknowledging the need for closed-access datasets to protect national security and proprietary information.

“I think you got to go back to basics, for me, number one is you’re going to have two types of databases. You’re going to have the open-source databases, and you’re going to have proprietary databases, you need both,” he said.

“But then you also need to have a computer, systems, capabilities, that have the ability to compute with very quiet supercomputers that a lot of people don’t have access to, probably in our national labs and so forth,” he added.

“But then you need another set of very, very capable systems that universities across this country can have access to, regardless of where you’re at. Because I don’t think we can make decisions, or learn as much information, with proprietary systems than we can with open systems, open databases, and allow a huge number of people to be able to have access to it.”

“You need both,” he emphasized.

Rounds also argued that advancements in health care from the use of AI will be a major driver for building public confidence in the emerging and rapidly evolving technology.

“What I tell folks is, if there was one thing that’s going to bring the American public in full support for the implementation of artificial intelligence, it’s going to be health care. I’m personally convinced based on what we’ve been able to learn,” he said, referring to a Defense Department classified briefing on the pandemic that included the use

continued on next page

In This Issue . . .

of AI to assess "healthcare issues."

"I believe that if we properly incorporate AI, into our health care and into the laboratories, we can cure the vast majority of cancers within a five-year period of time," Rounds predicted to underscore his point in remarks that overall emphasized the potential benefits of AI.

DHS, civil society advocates look ahead to national security memo required under AI order

Posted May 7, 2024

With final guidance for agencies on procuring artificial intelligence products and services still to be resolved, officials from the Department of Homeland Security and major civil society groups have started examining the next agenda item of President Biden's executive order on AI — an interagency memo on rights impacting national security systems.

"One big thing that we're kicking off in earnest — which is broader than DHS — is that we're going to be working on the national security memorandum that's required in the executive order," Iranga Kahangama, DHS' assistant secretary for cyber, infrastructure, risk, and resilience, said at a recent event hosted by the Center for Security and Emerging Technology.

Kahangama was responding to a question about what's next in the timeline under the EO, section 4.8 of which calls on the assistant to the president for national security affairs and the assistant to the president and deputy chief of staff for policy to oversee an interagency process culminating in the submission of a national security memorandum to the president within 270 days of the Oct. 30 order.

That memo should be made public, the Brennan Center for Justice wrote in an April 9 post noting — despite declarations to the contrary — that, "The Biden administration's AI approach leans far too heavily toward secrecy."

The memorandum, which the EO says "shall outline actions for the Department of Defense, the Department of State, other relevant agencies, and the Intelligence Community, to address the national security risks and potential benefits posed by AI" would apply to "AI when it is used as a component of a national security system."

Such uses were not covered under the March 28 memo the Office of Management and Budget released to guide federal agencies' implementation of the executive order. And as civil society groups weigh in on the particulars of AI procurement policy in response to a request for information from OMB, the advocates are also calling for greater transparency regarding the national security memorandum.

Among other things, the Brennan Center post calls for clearly defined criteria for classifying AI systems as national security components and procedures for relevant agencies to maintain detailed inventories of such systems.

"Transparency is one of the core values animating White House efforts to create rules and guidelines for the federal government's use of AI," the Brennan Center wrote. "But exemptions for national security threaten to obscure some of the most high-risk uses of AI: for example, determining who is surveilled, who is questioned and searched at the airport, who is placed on watchlists, and even who is targeted using lethal force."

As with the OMB memo, the EO notes the national security memo should aim to manage the risks using AI can pose to the rights or safety of US individuals. "In appropriate contexts," the EO adds, the national security memo should also address risks to the rights and safety of "non-United States persons."

April 29 comments the Brennan Center submitted to OMB along with the Electronic Privacy Information Center and other civil society groups highlighted that some of the more concerning AI use cases cited in the agency's March 28 memo as potentially rights impacting may not be covered under that document but in the forthcoming national security memo. The comments called for clarity from OMB and the national-security related agencies.

"For dual use systems, such as systems procured to collect domestic intelligence and initiate criminal investigations, OMB should clarify how its guidance would apply," the groups wrote. "Both OMB and agencies that rely on dual use systems should make every effort to ensure that procurement of these systems aligns with the procurement standards

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.

OMB establishes to protect privacy, civil rights, and civil liberties."

The groups' comment featured an example of using AI to monitor social media for security threats, which, as the Brennan Center separately noted in January, is a high-profile use case of the technology at DHS.

The groups — arguing along with others who submitted comments to OMB — for a needs assessment to occur before any AI solicitation, note the ineffectiveness of such programs.

"Not only is evidence of their utility lacking, they have also led to wrongful and discriminatory arrests, interrogations and investigations, and chilling effects on online expression," the groups wrote. "This analysis alone should lead agencies to halt procurement."

The example is of relevance with the Israel-Palestine conflict dragging on as federal elections approach.

"Agencies should assess how racial and ethnic biases embedded in natural language processing, the machine-learning process underlying many social media monitoring tools, would amplify harms to marginalized populations that are already disproportionately scrutinized, such as Black, Latino and Muslim communities," the groups wrote.

Diving a little deeper, they acknowledge: "Sentiment analysis tools that are programmed to always associate neutral sentiment with a specified list of identity terms representing protected characteristics (e.g., 'gay,' 'Muslim,' and 'feminist') may lower the risk of discrimination compared to tools that lack such a feature."

"Ultimately, however, vendors' provision of technical safeguards should not displace agency judgment that this technology is far too inaccurate for deployment in law enforcement and other high-risk contexts," they said. "In particular, sentiment analysis conducted on non-Latin derived languages, such as Arabic and Urdu, is likely unreliable and error prone given the lack of high-quality web data on such languages (the most common source of training data for large language models)."

In a real-world example of the harmful associations such AI systems can make, the Brennan Center's January post noted, "Instagram users recently found that the label ['terrorist'] was added to their English bios if their Arabic bios included the word 'Palestinian,' the Palestinian flag emoji, and the common Arabic phrase 'praise be to god.'"

"Bias in algorithmic tools has long been a concern, ranging from predictive policing programs that treat Black people as suspect to content moderation practices disfavoring Muslim speech," the group wrote, adding, "Generative AI also exacerbates longstanding problems."

Collaboration on AI factors into State Dept.'s cyberspace and digital policy strategy

Posted May 7, 2024

The Department of State has released an international cybersecurity and digital strategy that pledges to work toward "digital solidarity" across a range of issues including the safe and secure deployment of artificial intelligence, under a directive from Congress to create a plan on global cyber engagement and tech diplomacy.

The U.S. will work "with any country or actor that is committed to developing and deploying technology that is open, safe, and secure, that promotes inclusive growth, that fosters resilient and democratic societies, and that empowers all people," Secretary of State Antony Blinken says in a foreword to the new strategy released May 6.

Blinken discussed the strategy in a May 6 speech at the RSA Security conference in San Francisco.

The strategy is based on three principles, the document says, including that State "will implement a comprehensive policy approach that uses the appropriate tools of diplomacy and international statecraft across the entire digital ecosystem," which includes AI among a host of elements such as software protocols, technical standards, cloud computing, and the Internet of Things.

The other principles say the State Department "will pursue an affirmative vision for cyberspace and digital technologies focused on delivering the benefits of technology and grounded in international commitments and international law, including international human rights law."

And, they say, State "will integrate cybersecurity, sustainable development, and technological innovation throughout our approach."

"In line with these three principles," the strategy says, "the Department of State will build digital solidarity through four areas of action, which flow from creating and governing digital ecosystems to defending against malicious actions and delivering assistance and building resilience:"

1. *Promote, build, and maintain an open, inclusive, secure, and resilient digital ecosystem.*
2. *Align rights-respecting approaches to digital and data governance with international partners.*
3. *Advance responsible state behavior in cyberspace, and counter threats to cyberspace and critical infrastructure by building coalitions and engaging partners.*
4. *Strengthen and build international partner digital and cyber capacity.*

Blinken says in the foreword, "We are rallying coalitions of governments, businesses, and civil society to shape the digital revolution at every level of the technology 'stack' — from building subsea cables and telecommunication networks, to deploying cloud services and trustworthy artificial intelligence, to promoting rights-respecting data governance and norms of responsible state behavior."

The strategy includes a section on "the future of AI technologies governance" that says, "AI technologies could be powerful tools for expanding knowledge, increasing prosperity and productivity, and addressing global challenges, and AI tools may help advance the seventeen" United Nations' sustainable development goals.

It says, "AI applications have the further potential to improve many aspects of citizens' lives including food security, health applications, good governance and democratic consolidation, and natural disaster preparedness and prevention."

But it warns, "The rapid growth of AI technology, however, comes with the significant risk that its use may exacerbate inequality and economic instability, stifle competition, cause consumer harm, aggravate discrimination and bias, invade privacy, enhance malicious cyber activity, and improve authoritarian capabilities for surveillance and repression."

It cites a series of challenges including "how we compensate for the uses of intellectual property as well as authenticate, label, or detect synthetic content. AI may also require workforce adaptations across economies; the rising energy demands of high-end AI chips and data centers could become a significant barrier to developing local capabilities."

On the security front, it says, "state and non-state actors have been observed using generative AI systems for malicious purposes, including to manipulate and disseminate disinformation at speed and scale. Many AI technologies are also dual use, lending themselves to new military and national security capabilities that may lack appropriate human rights and civil liberty protections and other safeguards."

In line with the strategy, "The United States is working with allies and partners to move quickly to address the ways in which artificial intelligence can potentially destabilize societies while preserving its benefits — and, crucially, staying true to democratic values and protecting human rights."

State says, "A critical part of this work is not only safeguarding an open and independent research environment but also partnering with emerging economies in the development and deployment of AI technologies. Helping to provide unrestricted access to an open, interoperable, reliable, and secure Internet while demonstrating how AI can serve a shared agenda across the globe can help reduce the risk that the AI revolution will contribute to global instability and diminish our ability to address global challenges."

The document notes ongoing work "at the G7, Global Partnership on Artificial Intelligence, the Council of Europe, OECD, UN, UNESCO, and other fora to manage the risks of AI and ensure its benefits are widely distributed."

"In addition," it says, "we will need to work together to invest in the science research and infrastructure necessary to measure, evaluate, and verify advanced AI technology systems."

OpenAI, Microsoft counter NY Times push for documentation in landmark copyright suit

Posted May 7, 2024

Defendants Microsoft and OpenAI are asking a federal court to impose some limits and restrictions on the documentation being sought by the New York Times in its landmark lawsuit accusing the companies of copyright violations from the training of its generative artificial intelligence models.

"As a threshold matter, Defendants have not unduly delayed negotiations over the orders at issue," write lawyers for the defendants in a May 3 response to the U.S. district court for southern New York in opposition to the Times' request for an order.

"While Plaintiff's recounting of the parties' exchanges may accurately list the dates of the parties' communications, it lacks important context," the response letter says.

"In particular, with respect to the last round of edits offered by Plaintiff, Defendants were unable to meet Plaintiff's arbitrary April 30 deadline only because Defendants wanted to streamline negotiations and present a single counterproposal, rather than a separate proposal from each Defendant," the lawyers for OpenAI and Microsoft argue.

At issue is access to internal documents and correspondence related to the development of ChatGPT and other generative AI. The Times argues the companies assigned its content a higher priority in the training process, and the documents are being sought in part to demonstrate those allegations.

In response, the defendants say the Times' request for a protective order and for electronically stored information is too expansive, and are offering alternative orders that would allow for the return of inadvertently produced privileged documents under a so-called "clawback" provision and the inclusion of an "editorial decision-making" category for "highly confidential documents" limited to review by in-house counsel, among other requests to the court.

"This provision is crucial because Plaintiff continues to report extensively on this litigation. Defendants recognize that The New York Times has a right to report the news," the defendants' lawyers argue in the letter.

"But it would be inappropriate for The New York Times' inhouse attorneys conducting, for example, prepublication review of reporting about Defendants to have access to Defendants' highly confidential information. There is too great a risk that Defendants' highly confidential information may be improperly used, even if inadvertently," the letter says.

"The Court should not allow Plaintiff to use the discovery process to transmit confidential information to its editorial staff," it adds.

The case, *New York Times Company v. Microsoft, OpenAI et al.*, is one of the most notable among a bevy of lawsuits filed since last summer against generative AI developers over alleged copyright violations. Since the Times lawsuit late last year, a number of other news groups have filed legal complaints against AI developers.

At the same time, the U.S. district court for southern New York on April 1 rejected a request by California plaintiffs against OpenAI to intervene in the New York 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.

Microsoft has accused the Times of failing to produce a "single real-world" example of ChatGPT violating its copyright protections, and instead is pushing hypothetical scenarios in its quest for a federal court to order the destruction of chatbots trained with copyrighted materials.

"The Times offers no solution for the Complaint's core deficiency: that it alleges not a single real-world instance of someone using the GPT-based products in a way that violates The Times's rights or harms its interests," Microsoft said in a March 25 memo to the court requesting that core portions of the landmark lawsuit be dismissed.

AI to play key role as Commerce announces CHIPS funding for 'digital twins' institute

Posted May 7, 2024

The Department of Commerce is standing up a manufacturing institute under the CHIPS and Science Act "focused on digital twins for the semiconductor industry," with a $285 million funding opportunity for a private-sector entity to run the "first-of-its-kind" institute.

"Unlike traditional, physical research models, digital twins can exist in the cloud, which enables collaborative design and process development by engineers and researchers across the country, creating new opportunities for participation, speeding innovation, and reducing costs of research and development," according to a May 6 Commerce announcement.

"Digital twin-based research can also leverage emerging technology like artificial intelligence to help accelerate the design of new U.S. chip development and manufacturing concepts and significantly reduce costs by improving capacity planning, production optimization, facility upgrades, and real-time process adjustments," Commerce said.

Commerce said the funding could go toward "operational activities to run the Institute; basic and applied research related to semiconductor digital twin development; establishing and supporting shared physical and digital facilities; industry-relevant demonstration projects; and digital twin-related workforce training."

The department explained, "The CHIPS for America Program anticipates up to approximately $285 million for a first-of-its kind institute focused on the development, validation, and use of digital twins for semiconductor manufacturing, advanced packaging, assembly, and test processes. The CHIPS Manufacturing USA institute is the first Manufacturing USA institute launched by the Department of Commerce under the Biden Administration."

Commerce said, "The CHIPS Manufacturing USA institute is expected to use integrated physical and digital assets to tackle important semiconductor-industry manufacturing challenges. By establishing a regionally diverse network, the institute will foster a collaborative environment to significantly expand innovation, bring tangible benefits to both large and small to mid-sized manufacturers, engage diverse communities, and ensure robust nation-wide workforce training."

Deadlines

The 81-page notice of funding opportunity from the National Institute of Standards and Technology calls for concept papers by June 20 and complete applications by Sept. 9.

NIST's CHIPS Research and Development Office will host a May 8 webinar on the program and hold a "Proposers Day" on May 16 "to promote awareness of this NOFO and provide a forum for organizations to identify prospective partners."

CHIPS Manufacturing USA Program director Eric Forsythe and deputy director Michael McKittrick will brief participants during the webinar, which requires registration in advance.

NIST says, "Eligible applicants for the Institute award are non-profit organizations; accredited institutions of higher education; State, local, and Tribal governments; and for-profit organizations that are domestic entities."

High-level enthusiasm

Leaders from the White House, Commerce and NIST made statements on the funding opportunity, underscoring its importance within the CHIPS implementation effort.

Arati Prabhakar, director of the White House Office of Science and Technology Policy, said, "Under President Biden's leadership, we're writing a new chapter in semiconductor manufacturing in America. CHIPS R&D is about making sure American manufacturers can continue to succeed and thrive. Digital twin technology can accelerate the costly and time-consuming work to develop the next generation of robust manufacturing for this extraordinarily complicated product."

Commerce Secretary Gina Raimondo said, "Digital twin technology can help to spark innovation in research, development, and manufacturing of semiconductors across the country — but only if we invest in America's understanding and ability of this new technology. This new Manufacturing USA institute will not only help to make America a leader in developing this new technology for the semiconductor industry, it will also help train the next generation of American workers and researchers to use digital twins for future advances in R&D and production of chips."

NIST Director Laurie Locascio said, "Digital twin technology will help transform the semiconductor industry. This historic investment in the CHIPS Manufacturing USA institute will help unite the semiconductor industry to unlock the enormous potential of digital twin technology for breakthrough discoveries. This is a prime example of how CHIPS for America is bringing research institutions and industry partners together in public private partnership to enable rapid adoption of innovations that will enhance domestic competitiveness for decades to come."

White House officials call for congressional action in announcing first NAIRR projects

Posted May 6, 2024

White House officials overseeing the National AI Research Resource program renewed calls for Congress to enact funding and authorization for the pilot program, at an event announcing a first round of several dozen research projects intended to guide the development of safe and secure AI technologies.

"Today marks a pivotal moment in the advancement of AI research as we announce the first round of NAIRR pilot projects," said National Science Foundation Director Sethuraman Panchanathan at a May 6 event.

"The NAIRR pilot, fueled by the need to advance responsible AI research and broaden access to cutting-edge resources needed for AI research, symbolizes a firm stride towards democratizing access to vital AI tools across the talented communities in all corners of our country," he added in a statement.

The NAIRR pilot project was launched in January under President Biden's Oct. 30 executive order with the goal of broadening access to the core research and resources for responsibly developing AI technologies by ensuring privacy and civil rights protections.

Panchanathan said "pilot" was a key word for the program and the announcement today of a first round of research projects, citing a pending legislative proposal to fully fund and implement the NAIRR to achieve its goals for democratizing AI development and research, which to date has been dominated by big tech firms, according to proponents of the program.

"But remember the word pilot, which means that it calls for a full-scale implementation rather soon," said Panchanathan at the May 6 White House event.

"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."

To that point, the Senate Commerce Committee is poised to mark up the CREATE AI Act — a bipartisan plan by Sens. Mike Rounds (R-SD), Todd Young (R-IN), Martin Heinrich (D-NM) and Cory Booker (D-NJ) — that would fully fund and authorize the NAIRR program.

Sens. Rounds, Young and Heinrich are co-leaders of Senate Majority Leader Charles Schumer's (D-NY) AI working group, and their proposal to support the NAIRR program is viewed as an important step for the federal government to harness the benefits and manage the risks of the emerging technology.

White House Office of Science and Technology Director Arati Prabhakar described the diverse range of the 35 projects to receive support under the NAIRR program as representative of the Biden administration's goal for both managing the risks and promoting the benefits of AI.

She countered arguments that AI safety and innovation are competing goals saying building out the AI systems being backed by the NAIRR program will help in identifying and mitigating potential risks.

"I want to finish by circling back to where I started, which was about AI risks and benefits," Prabhakar said at the event.

"And a question I get asked all the time, I'm sure you all get it too, is the question of the conflict between safety and innovation. And I actually just think it's the wrong framing of the situation," she said.

"Because building and using AI is how we are going to understand its risks, and it's how we're going to learn how to make more and more effective and safe and trustworthy AI systems. So, our job really is to be vigorous and nimble in managing AI's risks, and at the same time to be vigorous and nimble in harnessing AI for its benefits," Prabhakar said in laying out the administration's AI research goals.

"And these things are going to go together," she said about managing risks and promoting AI benefits.

"Projects granted computing allocations in this initial round encompass a diverse range of AI-related areas, including investigations into language model safety and security, privacy and federated models, and privacy-preserving synthetic data generation. Other projects also focus on domain-specific research, such as using AI and satellite imagery to map permafrost disturbances, developing a foundation model for aquatic sciences, securing medical imaging data and using AI for agricultural pest identification," says the NSF statement announcing the new research projects.

Prabhakar and Panchanathan also announced the process for submitting and selecting a second round of projects under the NAIRR program.

"In tandem with the announcement of initial awards, the NAIRR Pilot opened the next opportunity for researchers and educators to apply for access to resources that support AI research, including advanced computing systems; cloud computing platforms; access to foundation models, software and privacy enhancing technology tools, collaborations to train models; and education platforms," according to the statement.

"This opportunity includes cutting-edge resources contributed by the pilot's nongovernmental partners, including Microsoft, Amazon Web Services, NVIDIA, SambaNova Systems, Cerebras, OpenAI, Anthropic, Groq, EleutherAI, OpenMined, Hugging Face and Vocareum."

"The second opportunity also seeks to connect educators and instructors in universities to computing, data, and software resources that will enable them to train their students through hands-on projects and exercises," according to the statement which encourages potential applicants to contact White House science officials at https://nairrpilot.org/.

White House officials also announced the release of a report by the President's Council of Advisors on Science and Technology which Prabhakar hailed as detailing the potential AI impacts for the scientific community.

"This new PCAST report delves into those and many other fields of research, to show what's going to be required to realize this potential for AI and research, how AI is going to change the practice of research itself, change the nature of science, and to really show us the dazzling possibilities that are had, if and when we can get this right," she said, adding "that's really what it's all about."

Consumer, industry groups identify need for clarity on FTC proposal to hold AI platforms liable for impersonation

Posted May 6, 2024

The Federal Trade Commission's proposal to extend liability in conjunction with impersonation fraud enabled by artificial intelligence to entities providing the technology is prompting calls by industry and consumer groups for the agency to further detail its plans.

"The FTC proposes to define an unfair or deceptive act or practices as the provision of 'goods or services with knowledge or reason to know' that goods or services will be used to commit impersonation fraud," read comments from the industry group TechNet. "However, by failing to define 'reason to know,' the FTC creates significant uncertainty for providers of innovative technology services."

The comments, along with those from almost a hundred others, were submitted on the April 30 deadline in response to the commission's supplemental notice of proposed rulemaking amid an increase in scams where fraudsters typically attempt to exploit victims by posing as relatives in need of money and use AI to effectively mimic their voices.

But while one chunk of the proposal — applying existing rules against impersonation to individuals in addition to businesses and governments — is uncontroversial, the uncertainty over how liability will apply to those behind the "means and instrumentality" for committing such fraud has even put some civil society groups on opposite sides of the debate.

"While we generally support the FTC's ability to use its statutory authority to prohibit the impersonation of individuals, we believe the proposed rule imposes significant, vague, and subjective burdens on innovators, including those in the Artificial Intelligence (AI) space," TechNet wrote.

In joint comments submitted with the Electronic Frontier Foundation, digital consumer advocates at Public Knowledge generally agreed, noting, "more specificity is needed in the language of the rule to ensure that general purpose tools, which may have the potential for misuse, are not unintentionally swept in by the regulation."

"Many technologies, including AI tools, have both lawful and unlawful applications," read the comments from EFF and Public Knowledge. "The standard of 'knowledge or reason to know' should be defined to require actual knowledge or willful ignorance of specific unlawful uses. This interpretation will ensure that the sellers and developers of general-purpose tools that may be misused by bad actors are not swept in by a too broad standard."

The call for liability to require "actual knowledge" of the fraud was also made by TechNet and industry groups like NCTA — The Internet and Television Association.

"Taken too broadly, the statement that '[o]ne who places in the hands of another a means of consummating a fraud or competing unfairly in violation of the Federal Trade Commission Act is himself guilty of a violation of the Act,' would apply to far too wide a range of behavior, and will hold sellers and makers of general-purpose tools liable for misuses they cannot control," EFF and Public Knowledge continued.

The groups said, "In many cases, tools cannot be fairly considered 'a means of consummating a fraud' as they have significant legitimate uses," and provided examples of how the rule could end up being counterproductive by disincentivizing the use of AI to identify fraud, in addition to depriving those who could use it to more easily participate in society.

"Consider the rise of AI technology, sometimes called "deepfakes," that can create realistic-appearing images of people, or copies of their voice," EFF and Public Knowledge wrote. "Technologies like this may be useful in many areas—for example, voice cloning technology is already deployed in iPhones as an accessibility feature for users with speech impairments."

They said: "An overly broad approach to 'instrumentalities' could harm the very constituencies the Commission seeks to protect. For example, AI tools that can be used to facilitate impersonation scams can also be used to protect users from these very scams … AI-powered identity verification systems can help prevent impersonation, AI-driven content moderation can identify and remove scam content from online platforms, and AI-based algorithms to detect phishing emails, fraudulent transactions or counterfeit products."

But another set of consumer groups — including the Consumer Federation of America, the National Consumer Law Center and the Electronic Privacy Information Center — argued that the difficulty of tracking fraudsters, and the overwhelming number and severity of cases, should justify the commission creating "financial incentives to discourage complicity and complacency among providers of products or services that could be used to facilitate impersonation scams."

"Actual knowledge alone is not an appropriate standard, as a company should have a strong financial incentive to investigate suspicious activity prior to obtaining actual knowledge that its offerings are being used to perpetrate fraud," EPIC and the other consumer groups wrote. "Where a provider fails to take action to prevent scams despite having received notice, or despite having access to data from which that provider should have detected fraudulent behavior, or despite having some other reason to suspect that their offerings have been used to facilitate scams, that failure to act should result in liability."

For a third set of consumer representatives — those at Consumer Reports — that should potentially mean going without the service altogether.

As part of a proposed "reasonableness standard," Consumer Reports wrote, "companies should marshal all the strategies at their disposal to prevent their tools from being used for fraud — including not offering a certain product in the first place — up and until the drawbacks to consumers of those strategies overcome the benefit of fraud reduction."

Consumer Reports suggested the reasonableness standard as a solution to the FTC's proposed language around the knowledge criteria for liability. Regarding companies' responsibilities if they suspect their offerings qualify as "means or instrumentalities" for impersonation fraud, the group said, there's "a bit of ambiguity."

Presidential advisory group backs data transparency for responsible purchasing of AI

Posted May 6, 2024

The National AI Advisory Committee is recommending robust guidelines for federal agencies on the management and transparency of data to ensure the responsible purchasing of artificial intelligence for government use.

"As a topic, the question of data standards and data transparency is foundational to understanding and regulating AI. Knowing what kind of data a model was trained on is pertinent to being able to deploy that model in a trustworthy manner," says a findings and recommendation document approved by NAIAC at its May 2 public meeting.

"As such, establishing minimum standards for data transparency for model developers, along with creating appropriate tools for dataset examination, would be an important component of creating a responsible AI ecosystem," the advisory group says.

To enable federal procurement officials to responsibly purchase AI technologies, NAIAC is recommending the White House Office of Management and Budget issue guidance for federal agencies on the handling and source of data.

OMB "should engage agencies, develop procurement guidance, and ensure periodic updating of data transparency standards," says the NAIAC recommendation document.

The NAIAC recommendation was released in the wake of OMB issuing a "request for information" on new purchasing requirements for responsible AI technologies. The OMB request was issued the same day it released final guidance to federal agencies on implementing President Biden's Oct. 30 executive order for safe and secure AI technologies.

NAIAC says its recommendation is intended to build on those ongoing and past OMB efforts for data management, including its recent final guidance on implementing Biden's order.

That OMB guidance told agencies to "secure documentation about the capabilities and limitations of AI systems and models through means such as data cards, as well as obtain information about the provenance of data used in training or fine-tuning AI," the NAIAC recommendation document notes.

"This effort builds on the Federal Data Strategy developed in the OMB M-19-18 memo, which articulated data governance practices for federal agencies, including data documentation, provenance, and standards," NAIAC notes. The 2019 OMB memo was issued to create consistency among agencies on data management practices with a focus on protecting security, privacy and confidentiality.

"First, OMB should pay careful attention to how agencies are implementing data transparency components of" its recent final guidance on Biden's EO "to develop best practices. Each agency should be encouraged to collaborate with a range of stakeholders involved in the provision and procurement of AI models, including academia, civil society, advocacy organizations, and industry (where legally and technically feasible) to examine best practices," NAIAC recommends.

"Such stakeholder consultation may lead to a consensus standard or customization of the standard for agency-specific practice. Either way, agencies should strive for the development of clear data transparency standards," the advisory group says.

"Second, OMB should build on existing federal policies and incorporate the relevant data transparency standards in its procurement guidance," the NAIAC recommendation document says, adding that any decisions "stemming" from OMB's recent RFI "should consider the tension between interoperability and customization of data transparency standards and requirements."

"Third, to ensure that data transparency standards remain relevant and effective, OMB and agencies should institute methods for periodic review and updating of these standards. Doing so will help adapt to technological advancements, maintaining the effectiveness of such standards and improving public trust," NAIAC recommends.

NAIAC approved its recommendation on AI procurement along with a series of other findings and recommendations on a range of topics including data transparency, protecting civil rights, AI safety, and setting standards for responsible government procurement of AI technologies. The advisory group also approved its second annual report at the May 2 meeting, in compliance with a congressional mandate.

NAIAC was created by the National AI Initiative Act of 2020 to advise the president and the National AI Initiative Office in the White House Office of Science and Technology Policy, according to the National Institute of Standards and Technology which facilitates the advisory group. The advisory committee consists of 26 experts on AI from industry, academia and other research groups. It held its first meeting in May 2022 and issued its first report in May 2023.

Tech group urges policymakers to back semiconductor research strategy in support of AI

Posted May 6, 2024

The Information Technology Industry Council is calling on federal policymakers to back up CHIPS and Science Act funding for domestic production of advanced semiconductors with sizable investments in research aimed at artificial intelligence development, which is also authorized under the CHIPS law.

"We urge U.S. policymakers to develop a national semiconductor R&D strategy that supports commercial R&D priorities and strengthens U.S technological competitiveness," ITI president and CEO Jason Oxman said in a May 2 blog post.

"The U.S. Congress must also stay involved," Oxman said, arguing that "lawmakers must provide sufficient funding for critical R&D and science programs for key technology focus areas, notably artificial intelligence, authorized under Division B of the CHIPS and Science Act."

He said key programs include the National Institute of Standards and Technology's Scientific and Technical Research Programs, the National Science Foundation's Directorate of Technology, Innovation and Partnerships, and the Department of Energy's Office of Science.

The Biden administration has been rolling out announcements of CHIPS Act grants for building new production facilities in the United States, including an April announcement of funding for Micron advanced memory chip projects in New York and Idaho.

Oxman praised that aspect of the CHIPS program, saying, "Since its enactment in 2022, over 50 new semiconductor ecosystem projects across 20 states totaling more than $200 billion in private investment and 40,000 new jobs have been created. These projects include building new fabs for manufacturing leading edge chips that power AI machine learning and everyday devices like laptops, cellphones, and household appliances."

Oxman said, "The law provides the necessary funding — including $39 billion direct support and up to 25%

investment tax credits — for companies to build new or renovate existing chip manufacturing facilities in the U.S. through the CHIPS Incentives Program, which is an essential part of long-term semiconductor leadership."

The next step, Oxman said, is a robust semiconductor R&D program authorized under CHIPS.

"The CHIPS and Science Act provides funding of up to $11 billion for four integrated entities, including the National Semiconductor Technology Center (NSTC), National Advanced Packaging Manufacturing Program (NAPMP), Manufacturing USA Institute and CHIPS Metrology to support chips R&D," he said.

"The CHIPS R&D program is guided by the Industrial Advisory Committee (established via the FY 2021 NDAA), which comprises leaders from a broad range of disciplines including the semiconductor industry and academia to advice on the CHIPS R&D programs. The U.S. Commerce Department has also announced notice of funding opportunities (NOFOs) for the Manufacturing USA Institute, NAPMP materials R&D, and metrology research," according to Oxman.

"While this is important progress, more work needs to be done to achieve an ambitious R&D program that keeps the U.S. in the lead," he said. "We urge U.S. policymakers to develop a national semiconductor R&D strategy that supports commercial R&D priorities and strengthens U.S technological competitiveness."

"In addition," Oxman said, "while the Biden Administration has allocated more than $5 billion for the NSTC consortium in February 2024, the administration should take steps to announce NOFOs for research and establish a headquarters for the NSTC — along with affiliated technical centers. Further, the administration should work with all stakeholders to support commercial R&D that will drive advancements in AI, quantum computing and advanced communications. This includes supporting key investments for the construction of commercial R&D facilities, in addition to the funding of the NSTC."

Oxman concluded, "The administration is doing an admirable job implementing the CHIPS programs. The U.S. Congress will continue to play an important role in overseeing the effective obligation of grant funds appropriated under Division A of the CHIPS and Science Act. We look forward to continuing our partnership with U.S. policymakers to advance the development of semiconductor technologies and enhance U.S. competitiveness."

AI advisory group examines 'safety' to guide NIST work under Biden executive order

Posted May 3, 2024

A presidential advisory group on artificial intelligence has approved recommendations on testing for and determining the safety of AI technologies, to help guide the National Institute of Standards and Technology in its efforts to "red team" systems under President Biden's executive order for safe and secure AI.

The National AI Advisory Committee approved its findings and recommendations on AI safety at its May 2 public meeting, calling for increased funding through NIST to conduct additional research while arguing that current red-team testing is insufficient to address the range of detrimental possibles from unsafe AI systems.

"Existing safety and risk mitigation practices, such as AI red-teaming performed on [large-language models], can help to identify technical exploits and vulnerabilities. But technical interventions, performed in isolation, are likely insufficient," the NAIAC recommendations say.

Red teaming occurs when ethical hackers are authorized to emulate the tactics of real-world attackers to identify system vulnerabilities.

"Given the dynamic nature of AI and its deployment across many high-impact sectors of society, it is unlikely that a strictly technical focus on system capability is sufficient to mitigate risk," the NAIAC recommendations document adds.

NAIAC says NIST's recently established AI Safety Institute "should approach AI safety as an expansive field, addressing (at least) technical model engineering and broader societal concerns, rather than focusing on a single aspect of safety."

Also, the "federal government should help to develop the empirical research base needed to advance the science of AI safety, from technical auditing for vulnerabilities to controlled human testing environments," the recommendations say.

The advisory group acknowledges the role that red-team testing and the adoption of NIST's AI risk management framework can play to ensure AI system safety, but that is not enough.

"At the same time, meaningfully advancing AI safety methodologies and the science of AI safety will require further substantial investments to progress a broad understanding of AI's risks, technical safeguards, and sociotechnical considerations," the advisory group says in its recommendations.

"The government should provide substantial funding through NIST, the U.S. AISI, the National Science Foundation, the National Institutes of Health, and other agencies as appropriate, to advance the measurement and evaluation of AI safety risks, both broadly and within specific use contexts," the recommendations document adds.

Biden's Oct. 30 executive order on AI tasked the Commerce Department through NIST to establish guidelines "including appropriate procedures and processes, to enable developers of AI, especially of dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems," among other tasks.

The NAIAC recommendations take a broad view on what constitutes AI safety and describe red-teaming as only one, albeit important, element of a broader strategy for harnessing the benefits and minimizing the risks of AI.

What constitutes AI safety is "expansive," the NAIAC document says. "It includes both low-capability and high-capability AI systems. It includes attention to both near-term and long-term risks. It includes attention to known harms to people such as bias and discrimination, as well as potential risks associated with [chemical, biological, radiological and nuclear] catastrophes. AI safety is relevant across a broad spectrum of risk and over a long runway of time."

"A narrow view of 'AI safety,' over-indexing on any one dimension of risk at the expense of others, will produce an incomplete view of safe AI systems," the NAIAC document says.

NAIAC approved its recommendations on AI safety along with a series of other findings and recommendations on a range of topics including data transparency, protecting civil rights and setting standards for responsible government procurement of AI technologies. The advisory group also approved its second annual report at the May 2 meeting, in compliance with a congressional mandate.

NAIAC was created by the National AI Initiative Act of 2020 to advise the president and the National AI Initiative Office in the White House Office of Science and Technology Policy, according to NIST which facilitates the advisory group. The committee consists of 26 experts on AI from industry, academia and other research groups. It held its first meeting in May 2022 and issued its first report in May 2023.

Civil society groups push for regulatory amendment in comments to OMB on AI procurement

Posted May 3, 2024

Civil society groups responding to a request for information by the Office of Management and Budget have joined forces in highlighting how artificial intelligence is different and why it should therefore prompt changes to the Federal Acquisition Regulation, with emphasis on a need to test systems before and after deployment for harms such as propagating bias against minorities.

"Explicitly call out responsible AI practices in the Federal Acquisition Regulations (FAR)," the Center for Democracy and Technology wrote in April 29 comments appending a more detailed report the group simultaneously released on the issue.

CDT's ask directly counters tech industry groups which told OMB current rules are sufficient for implementing President Biden's executive order — EO 14110 — on "the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." Those groups noted FAR provisions requiring agencies to default to commercial products and services and associated "quality assurance" measures conducted by vendors.

"Any amendments [to the FAR] would likely be useful if they provide specific references back to requirements in [Executive Order 14110, OMB Memorandum M-24-10, Executive Order 14091], and any applicable statutes, as well as guidance provided in NIST's AI Risk Management Framework and the Blueprint for an AI Bill of Rights," CDT wrote in its comments.

EO 14091, issued February 2023, on "Further Advancing Racial Equity and Support for Underserved Communities," instructs federal agencies to "[protect] the public from algorithmic discrimination."

But as the CDT report notes, agencies are also encouraged under laws like the AI in Government Act of 2020 to adopt the technology. And — even as the civil society groups celebrate OMB's memo on implementing the more recent EO for noting the use of systems that fail to meet minimum requirements for protecting rights and safety should be discontinued — agencies like the Department of Homeland Security are interpreting the administration's policy approach as seeking to ease greater AI acquisition.

During a recent event, a senior DHS official noted greater use of Microsoft's Copilot and other trials of the technology across the department "as we relax, or implement our AI policies to allow the workforce to use these tools."

Against this backdrop, the first line of CDT's report titled "The Federal Government's Power of the Purse: Enacting Procurement Policies and Practices to Support Responsible AI Use" notes that already, "Government spending on artificial intelligence has reached unprecedented levels. In fiscal year 2022, the United States government awarded over $2 billion in contracts to private companies that provide services that rely on AI, and total spending on AI has increased nearly 2.5 times since 2017."

But while the industry groups argue there's nothing special about AI that should change the acquisition rules, CDT's report cited the NIST AI Risk Management Framework "to identify unique procurement challenges presented by AI."

"As NIST recognizes, datasets used to train AI systems may become detached from their original and intended context or may become stale or outdated relative to the deployment context," the report reads. "This is a particular challenge because procurements are often structured toward the creation of long-term contracts (typically, 5 years). Re-training AI will need to be built into procurements. If agencies procure systems from other agencies, this may add to the risk of systems becoming detached from their intended contexts."

CDT's comments reference this in highlighting the "quality assurance" provisions of the FAR for amendment.

"Because of the specific risks associated with 'drift' (the ongoing efficacy and suitability of an AI model over time), there may be particularly useful changes in Part 46 (Quality Assurance) because traditional rules around acceptance — 'acknowledgement that the supplies or services conform with applicable contract quality and quantity requirements' — may not be sufficient to manage AI risks."

The group added, "Although post-award management is a critical part of the acquisition process, most government contracts emphasize pre-award actions and contract formation rather than the continuous post-award monitoring, evaluation, and model refinement required for responsible AI."

"However, the risks associated with responsible AI practices are critical to monitor and address throughout post-award activities," CDT wrote noting that "Both NIST and [the Government Accountability Office] have warned about the need for meaningful post-award monitoring because 'AI systems may require more frequent maintenance and triggers for conducting corrective maintenance due to data, model, or concept drift.'"

Calling for a technical standard that agencies can use to conduct AI impact assessments that builds on NIST's work — such as SP 800-53 which relates to privacy and security for information — CDT's comments also reference those jointly submitted to OMB by the Electronic Privacy Information Center and the Brennan Center for Justice.

Those groups referenced EPIC's work with the Institute of Electrical and Electronics Engineers on a forthcoming AI procurement standard and offered an interim fix while also calling for changes to the FAR.

"Ideally, FAR should be amended to incorporate the OMB guidelines," the joint comments read. "In the meantime, agency Contracting Officers (COs) should designate these guidelines as a special responsibility standard under the Regulation. Section 9.104-2 authorizes COs to develop 'special standards of responsibility' with the 'assistance of appropriate specialists' when these are necessary for a 'particular acquisition or class of acquisitions.'"

"Vendors must show that they can fulfill these standards before a contract is awarded," EPIC and the Brennan Center for Justice wrote noting AI purchasing should be considered a "class of acquisitions."

CDT, EPIC, the Brennan Center, and the Lawyers' Committee for Civil Rights Under the Law — which submitted separate comments — all stressed the need for pre-award evaluations and post-award impact assessments.

The comments contain numerous examples of bias resulting in harms to minorities from AI systems already in use, including by the government.

Presidential advisory group debates AI-powered analysis of police body-cam footage

Posted May 3, 2024

The National AI Advisory Committee is developing recommendations on deploying artificial intelligence to analyze the often controversial use of body-worn cameras by local police and the resulting video footage, as some committee members raise concerns about potential privacy violations and the need to limit access to the growing volume of such footage.

"From our perspective, it's odd to pour that much money, that much investment into a camera, where you're paying for the camera, but not for the ability to analyze what the camera is picking up," said Stanford University professor Jennifer Eberhardt in her presentation of the proposed recommendation at a May 2 public meeting of the committee.

Eberhardt is a member of the NAIAC's law enforcement subcommittee and led the working group that developed the recommendations.

"And it seems to me that that's the whole purpose of the camera is to be able to better understand these interactions, to better understand how they unfold to be in a position to develop trainings that improve police community interactions, that would improve police community relations more broadly," she added to explain the reasoning behind the apparently controversial proposal.

Her presentation prompted what Eberhardt described as a "lively" discussion, with committee members voicing concerns about privacy and the ability to reidentify subjects in the videos despite efforts at anonymization. Also, there were concerns raised about widespread public access to the police camera footage by creating a national repository for the purposes of research and analysis.

In response, Eberhardt stressed that the purpose of the proposal was not to allow public access to the video footage, but to distribute the analyses to promote public awareness and improve overall policing.

One committee member proposed assigning the National AI Research Resource, a pilot research exchange hub developed under a White House task force report, the role of ensuring secure access to the proposed video repository, which Eberhardt embraced as a viable option.

The committee, however, tabled the proposal for further consideration at its next public meeting in the next month or so.

"To address the under-utilization of police body-worn cameras for research purposes, the federal government should invest in the development of statewide repositories of body-worn camera footage that academic researchers could access and analyze," says the draft recommendation presented to the committee.

"As a condition of receiving the grants, agencies and researchers should present detailed proposals for minimizing risks, including, but not limited to: data security, data access procedures and credentialing for researchers, officer privacy, privacy of members of the public, procedures as researcher review surfaces," the recommendation says.

The recommendation, "Encourage the Creation of Statewide Repositories for Police Body-Worn Camera Footage," was developed in part in response to the growing volume of police camera footage as many local law enforcement agencies adopt policies requiring the use of bod-worn cameras, at the urging of federally funded assistance grants, with the intention of establishing accountability.

But that growing amount of footage is not being leveraged for the purpose of overall improved policing, but rather is relied upon for specific instances and on a case-by-case basis, Eberhardt noted.

"Fortunately, with the rapid development of AI systems, there is a computational solution," the draft recommendation says. "Indeed, the primary strength of AI systems is their ability to find patterns in huge amounts of data."

The draft recommendation notes that, to date, the NAIAC subcommittee has focused on the regulation and use of AI tools to assist in countering crime such as the use of facial recognition systems, automated license plate readers and forensic ballistic analysis.

"Yet the computational analysis of officers' own body-worn camera footage is another use case that could be quite powerful — especially in communities where trust in police is low. Imagine a world where AI could offer more than sophisticated tools to solve crime, where we are offered data-informed approaches to healing decades-old rifts between the police and the public," the proposed recommendation argues.

"And with our eyes trained on the future, AI could be used to examine changes in the health of police-community relations over broad stretches of time — when crime begins to rise or fall, when the economy is humming or stalling, or when a critical incident, once again, captures the attention of the nation."

According to the proposal, a benefit of computational analysis of video footage "is that it does not require officers themselves to do anything that would take them away from their day-to-day jobs. Data collection is passive — and continuous. Why not leverage it?"

The committee did unanimously approve its second annual report at the conclusion of its May 2 meeting.

Also, the committee approved with some edits several recommendations and "findings" by various working groups including on reporting high-risk uses of AI, harnessing AI benefits for scientific developments, promoting data transparency, establishing standards for government AI procurement, protecting civil rights, and defining AI safety under Biden's executive order for safe and secure AI.

Transportation Dept. probes potential roles for AI, targets for advanced research

Posted May 3, 2024

The Transportation Department's research agency is asking for input on how artificial intelligence can be employed in the transportation sector and where to focus research efforts, as DOT moves to meet its assignments under an executive order.

DOT's "Advanced Research Projects Agency - Infrastructure (ARPA-I) is seeking input from interested parties on the potential applications of artificial intelligence (AI) in transportation, as well as emerging challenges and opportunities in creating and deploying AI technologies in applications across all modes of transportation," according to the DOT request for information published in the May 3 *Federal Register*.

"The purpose of this Request for Information (RFI) is to obtain input from a broad array of stakeholders on AI opportunities, challenges and related issues in transportation" under the direction of President Biden's Oct. 30 executive order on AI, DOT says.

DOT describes "a range of activities and efforts" underway at the department and lists 22 "potential areas for funded AI research and development" ranging from pedestrian safety to "real-time AI-based decision support tools, optimization and control of wide area traffic systems and transit operations."

It says, "Beyond transportation-specific use cases, AI also has the potential to increase operational efficiencies for DOT's own internal core business, regulatory, and permitting functions, including such applications as analyzing consumer complaints, compiling and summarizing public comments, streamlining permitting and application processes and more."

The RFI includes specific questions grouped in five areas: "current AI applications in transportation"; opportunities presented by AI; challenges presented by AI; autonomous mobility ecosystems; and "other considerations in the development of AI for transportation."

DOT asks stakeholders to link AI opportunities to the department's priorities "including safety, climate and sustainability, equity, economic strength and global competitiveness, and transformation."

Likewise, it asks for feedback on "risks presented by the use of AI in transportation and potential barriers to its responsible adoption," and again asks for connections to DOT priorities.

On "Autonomous Mobility Ecosystems," it asks, "What are the opportunities, challenges, and risks of AI related to autonomous mobility ecosystems, including software-defined AI enhancements? Describe how AI can responsibly facilitate autonomous mobility, including specifically safety considerations."

It says other "considerations may include ones such as potential priorities in transportation-specific future AI R&D funding, access to transportation datasets, the development of AI testbeds, physical and digital infrastructure needs and requirements, and workforce training and education."

Biden's science advisors urge broader access to federal datasets under AI order

Posted May 2, 2024

President Biden's science advisors are recommending providing access to federal datasets to a broader range of researchers under an executive order for safe and secure artificial intelligence technologies.

The recommendation by the President's Council of Advisors on Science and Technology is focused on a national AI research exchange hub established as a pilot project by the White House that would be formally authorized under a leading AI policy proposal in the Senate.

"Extensive support for widely accessible shared models, data sets, benchmarks, and computational resources is essential to ensuring that academic researchers, national and federal laboratories, and smaller companies and non-profit organizations can use AI to create benefits for the nation," says a recent PCAST report to the president dated April 2024.

To achieve those data goals, the report calls for an "expeditiously expanded" National AI Research Resource, or NAIRR, launched in January as a pilot by the National Science Foundation under a recommendation in a congressionally mandated White House task force report.

"PCAST recommends that the NAIRR pilot be expeditiously expanded to the scale envisioned by the NAIRR Task Force and fully funded. The full-scale NAIRR, together with industry partnerships and other AI infrastructure efforts at both the federal and state levels, could serve as a stepping stone towards AI infrastructure projects at the national or international level to facilitate high-impact research," the report says.

"The benefits of allowing limited, secure access to federal data sets by approved researchers, as well as allowing the release of carefully anonymized versions of such data sets to curated resource centers such as NAIRR, are immense," the report adds.

"PCAST strongly encourages expansion of existing pilot programs for secure data access and the development of guidelines for federal database management that incorporate cutting-edge privacy protection technologies as they become available," the report says among its recommendations.

The PCAST report will likely provide a boost for a Senate bipartisan proposal, the CREATE AI Act, to fund and authorize the NAIRR pilot project. The bill was slated for markup by the Commerce Committee on May 1, but that session was postponed amid the Senate's floor debate on Federal Aviation Administration reauthorization legislation which also falls under the committee's jurisdiction.

Also, the report is a boost to Biden's AI policy agenda by supporting an expansion of White House initiatives on researching safe and secure uses of AI.

"Many public and private sector activities addressing these issues are already underway, including government efforts tasked under the October 2023 Executive Order on AI," the report says referencing the Biden order that called for the PCAST recommendations.

"Reproducibility and validation are key principles underlying scientific integrity and the scientific method and must continue to be held at high value as we develop a culture of responsible AI use and expert human supervision of AI applications," the report says.

Specifically, the PCAST report offers a series of five recommendations including the expansion of the NAIRR pilot program and broader access to federal datasets.

"Adopt principles of responsible, transparent, and trustworthy AI use throughout all stages of the scientific research process," the report says among its recommendations.

"Managing the risks of inaccurate, biased, harmful, or non-replicable findings from scientific uses of AI should be planned from the initial stages of a research project rather than performed as an afterthought," the recommendation says.

"Support both basic and applied research in AI that involves collaborations across academia, industry, national and federal laboratories, and federal agencies as outlined in the vision for the NAIRR developed by the NAIRR Task Force," the report offers as another recommendation.

The recommendation calls on "funding agencies [to] broaden their postures regarding how to work with industry and which researchers can be supported in order to facilitate innovative research efforts and collaborations among different sectors."

And lastly, the PCAST report encourages "innovative approaches to integrating AI assistance into scientific workflows."

"The objective should not be to maximize the amount of automation, but to allow human researchers to achieve high quality science that utilizes AI assistance responsibly," the recommendation says.

Senators examine China’s AI efforts at global threats hearing with DNI Haines

Posted May 3, 2024

Senate Armed Services Committee members focused on artificial intelligence-related threats from China in the open portion of a hearing to review the intelligence community’s 2024 global threat assessment with Director of National Intelligence Avril Haines.

The committee heard from Haines and Lt. Gen. Jeffrey Kruse, director the Defense Intelligence Agency, at a May 2 hearing on the annual threat report. The committee also held a closed session to discuss sensitive aspects of the report with the witnesses.

The unclassified version of the report was released in March by the Office of the Director of National Intelligence.

Haines last month discussed the report with the House and Senate Intelligence panels, saying AI technologies will exacerbate threats from China and Russia.

Chairman Jack Reed (D-RI) in his opening statement said, “Beijing has sought ways to achieve its national objectives while avoiding a direct confrontation with the United States military,” including through investment in “offsetting technologies” such as artificial intelligence.

Haines observed that Chinese President Xi Jinping “is counting on China’s investments in technologies such as advanced manufacturing and robotics, artificial intelligence, and the high performance computing to drive productivity — productivity gains and spur growth in the future, yet he is increasingly concerned about the United States ability to interfere with China’s technological goals.”

“Moreover,” she said, “the PRC also remains focused on achieving its regional and global ambitions, which warrants, from their leadership’s perspective, a strategy that boosts China’s indigenous innovation and technological self-reliance, supports efforts to acquire, steal or compel the production of intellectual property and capabilities, and controls critical global supply chains that provide the leverage to achieve certain geopolitical outcomes to their advantage.”

In the military sphere, she said, the People’s Liberation Army is expected to “field more advanced platforms, deploy new technologies, grow more competent in joint operations, and seek to strengthen their nuclear forces and cyber capabilities, while also seeking to divide us from our allies in Europe and in the Indo-Pacific.”

Kruse briefly discussed how the U.S. intelligence community is using AI tools to improve efficiencies in collection and analysis, and offered to discuss in closed session efforts to counter the uses of AI by adversaries.

He said adversaries were showing “rapid growth in malign use of advanced technology, artificial intelligence, biotechnology, unmanned systems or cyber,” as well as “a growing number of adversaries who are interacting and partnering in ways and toward ends that we have not seen before.”

Sen. Jeanne Shaheen (D-NH) raised the question of election interference and said, more broadly, “Russia and China are using AI to improve their capabilities to reach into Western audiences.”

‘First of all,” she asked Haines, “are you able to share information with state and local officials when you see those kinds of AI or cyber generated influence into what’s happening in states?”

Haines said that, “working with [the Cybersecurity and Infrastructure Security Agency], what we’ve been doing is, in fact, been trying to expand our capacity to do so. But we do have direct communication with them on basically deepfakes and other types of manipulated media.”

Shaheen asked whether “our adversaries [are] using AI platforms in the United States to conduct disinformation and spread propaganda,” and drilled down to explore whether China or Russia were using AI tools to manipulate campus unrest related to the situation in Gaza.

Haines responded, after a choppy back and forth with the senator, “I am not seeing information that indicates that the Chinese government is directing that.”

Industry group asks Commerce to narrow definition of ‘large AI model’ in implementing Biden order

Posted May 2, 2024

An overly broad definition of a key term in President Biden’s executive order on artificial intelligence that is aimed at deterring the use of U.S. cloud companies to train models that could be employed for malicious cyber activity might end up harming use of the technology for public benefit, a major industry group told the Commerce Department.

“The Alliance urges the Department to take a more targeted approach to defining covered large AI models,” the Alliance for Trust in AI wrote in April 29 comments to Commerce’ Bureau of Industry and Security.

The comments are in response to a notice of proposed rulemaking BIS issued in accordance with the Oct. 30 executive order. Section 4.2 of the EO, among other things, instructs Commerce to propose regulations requiring U.S. infrastructure-as-a-service providers to report when foreign persons initiate transactions to train a “large AI model with potential capabilities that could be used in malicious cyber-enabled activity.” That is shortened to “large AI model” in the NPRM.

Spelling out potential civil and criminal penalties for non-compliance, the NPRM lists a host of information, ranging from the name and address of the individual or entity entering the transaction to the expected start and end date of the training run and "information on the training practices including the model of the primary AI used in the training run accelerators," which the infrastructure providers must report to Commerce within 15 days if they suspect it is a covered transaction.

The NPRM defines a "large AI model with potential capabilities that could be used in malicious cyber-enabled activity" as "any AI model with the technical conditions of a dual-use foundation model or otherwise has technical parameters of concern, that has capabilities that could be used to aid or automate aspects of malicious cyber-enabled activity, including but not limited to social engineering attacks, vulnerability discovery, denial-of-service attacks, data poisoning, target selection and prioritization, disinformation or misinformation generation and/or propagation, and remote command-and-control of cyber operations."

The industry comments acknowledge that "dual-use" is further defined in the proposed rule and EO to reflect a much more limited set of AI models, but, they said, "by including 'or has technical parameters of concern' and any 'capabilities that could be used to aid or automate aspects of malicious cyber-enabled activity' — rather than 'high levels of performance at tasks that pose a serious risk' — the proposed definition could include any general-purpose AI model, regardless of what it is trained for."

"For example," the group wrote, "an AI model trained to generatively fix grammar and spelling mistakes could be used to create content for phishing campaigns. This definition cannot be used effectively to differentiate between models that do or do not pose a risk of being used to enable malicious cyber activities in meaningful ways."

The comments also point out that a set of crucial factors have yet to be articulated at all for describing covered transactions and ask the agency to continue working with stakeholders on what those should be under the new rule.

"The NPRM notes that the Secretary will, in the future, publish a set of technical conditions as an interpretive rule under which a large AI model will be considered to have these capabilities. The Alliance urges the Secretary to engage stakeholders further in crafting these technical conditions to ensure that they are well scoped to capture AI models that could pose heightened risk without being overbroad," the group wrote.

They also argued that "a risk-based, contextual approach to safety can also help ensure that undue burdens are not placed on developers," and that harms from AI flow from how the technology is used and are not inherent to the training process.

"The majority of risks from AI models occur through downstream deployment and use by third parties, which developers cannot control; therefore, heavily regulating the developers and their models will increase regulatory burdens without meaningfully reducing risk," the group wrote, adding "This in turn will likely slow the pace of innovation and development of AI for good."

Sens. Warner, Tillis offer bill to bolster tracking of AI-powered cybersecurity incidents

Posted May 2, 2024

Senate Intelligence Chairman Mark Warner (D-VA) and Sen. Thom Tillis (R-NC) have introduced a bill to leverage and supplement existing cybersecurity vulnerability disclosure and tracking programs for use in the artificial intelligence realm, with provisions including a new "voluntary database to record AI-related cybersecurity incidents including so-called 'near miss' events," according to the senators.

The bill, the "Secure Artificial Intelligence Act," was introduced May 1 and aims to "improve the tracking and processing of [AI] security and safety incidents and risks" with an eye toward addressing key differences between AI systems and "traditional" software systems, according to a joint release from the two senators.

"Specifically, this legislation aims to improve information sharing between the federal government and private companies by updating cybersecurity reporting systems to better incorporate AI systems," the release says.

The measure includes roles for the National Institute of Standards and Technology, the Cybersecurity and Infrastructure Security Agency and the National Security Agency, and emphasizes collaboration with industry and voluntary private-sector participation.

"When it comes to security vulnerabilities and incidents involving artificial intelligence, existing federal organizations are poised to leverage their existing cyber expertise and capabilities to provide critically needed support that can protect organizations and the public from adversarial harm," a summary of the bill says.

"The Secure Artificial Intelligence Act ensures that existing procedures and policies incorporate AI systems wherever possible — and develop alternative models for reporting and tracking in instances where the attributes of an AI system, or its use, render existing practices inapt or inapplicable," it says.

The summary explains, "As NIST notes in their AI Risk Management Framework, AI risks differ from traditional software risks in key ways — including increased opacity and barriers to reproducibility, complex and non-deterministic system dependencies, more nascent testing and evaluation frameworks and controls, and a 'higher degree of difficulty in predicting failure modes' for so-called 'emergent properties' of AI systems."

The summary says the measure:

• *Requires NIST to update the [National Vulnerability Database] and requires CISA to update the [Common Vulnerabilities and Exposures] program or develop a new process to track voluntary reports of AI security vulnerabilities.*

• *Establishes a public database to track voluntary reports of AI security and safety incidents.*

• *Creates a multi-stakeholder process that encourages the development and adoption of best practices that address supply chain risks associated with training and maintaining AI models.*

• *Establishes an Artificial Intelligence Security Center at the NSA to provide an AI research test-bed to the private sector and academic researchers, develop guidance to prevent or mitigate counter-AI techniques, and promote secure AI adoption.*

"As we continue to embrace all the opportunities that AI brings, it is imperative that we continue to safeguard against the threats posed by — and to — this new technology, and information sharing between the federal government and the private sector plays a crucial role," Warner said in a May 1 statement.

"By ensuring that public-private communications remain open and up-to-date on current threats facing our industry, we are taking the necessary steps to safeguard against this new generation of threats facing our infrastructure," he said.

Tillis said, "Safeguarding organizations from cybersecurity risks involving AI requires collaboration and innovation from both the private and public sector. This commonsense legislation creates a voluntary database for reporting AI security and safety incidents and promotes best practices to mitigate AI risks. Additionally, this bill would establish a new Artificial Intelligence Security Center, within the NSA, tasked with promoting secure AI adoption as we continue to innovate and embrace new AI technologies."

According to the bill text, NIST within 180 days would be required to:

1. *initiate a process to update processes and procedures associated with the National Vulnerability Database of the Institute to ensure that the database and associated vulnerability management processes incorporate artificial intelligence security vulnerabilities to greatest extent practicable; and*

2. *identify any characteristics of artificial intelligence security vulnerabilities that make utilization of the National Vulnerability Database inappropriate for their management and develop processes and procedures for vulnerability management for those vulnerabilities.*

It would require NIST in coordination with CISA within one year to "develop and establish a comprehensive, voluntary database to publicly track artificial intelligence security and artificial intelligence safety incidents."

Among other provisions, CISA is directed within 90 days of enactment to convene "a multi-stakeholder process to encourage the development and adoption of best practices relating to addressing supply chain risks associated with training and maintaining artificial intelligence models."

The process would leverage efforts of the CISA-directed Information and Communications Technology Supply Chain Risk Management Task Force "to the greatest extent practicable."

The release notes endorsements from IBM, the Information Technology Industry Council and the Center for AI Policy.

Free speech concerns may shape Senate Judiciary panel bill for regulating AI replicas

Posted May 2, 2024

A Senate Judiciary subcommittee was told that free-speech rights could run afoul of a pending legislative proposal for extending copyright restrictions on audio and visual replicas produced by artificial intelligence, as senators eye revisions with the hope of moving the landmark legislation later this year.

"Congress is now considering whether to legislate a new federal right to bar the unauthorized replication of individuals' (including actors' and recording artists') likenesses and voices," Motion Picture Association general counsel Ben Sheffner noted in his testimony to the Senate Judiciary subcommittee on intellectual property.

"Enacting new legislation to address specific harms from the misuse of digital replicas likely can be done consistent with the First Amendment. But it will take very careful drafting to accomplish the goal of addressing these harms without inadvertently chilling legitimate, constitutionally protected uses of technologies," Sheffner said about AI which his industry is legitimately using to enhance its storytelling prowess.

Ben Sheffner, General Counsel, Motion Picture Association

His and other testimony offered at an April 30 subcommittee hearing were intended to guide senators in fleshing out the details of a "discussion draft" bill, the NO FAKES Act, unveiled in September. Chairman Chris Coons (D-DE) and ranking member Thom Tillis (R-NC) are co-sponsors of the bipartisan proposal, along with Sens. Marsha Blackburn (R-TN) and Amy Klobuchar (D-MN), who say they plan to move the bill through the committee later this year.

Coons and Tillis said at the hearing that they plan to formally introduce the NO FAKES Act this month, to get the committee process going.

And the free-speech issues raised at the hearing underscore the challenges faced by the senators as they seek to navigate these and other concerns about regulating AI activities, with implications for AI-related legislation beyond the subcommittee.

Senate Majority Leader Charles Schumer (D-NY) has tasked the chairs of all committees to consider the AI implications of legislative proposals working their way through the chamber.

"My testimony will summarize the vital First Amendment issues implicated by a potential federal statute creating a 'digital replica' right, emphasizing that creation of such a law would constitute a content-based regulation of speech, subjecting it to strict scrutiny, which requires both the existence of a compelling state interest to justify the regulation and narrow tailoring to serve that interest," Sheffner told the subcommittee.

"A federal digital-replica right must serve a compelling government interest," he told the subcommittee. And "any federal digital-replica right must be narrowly tailored," he added.

"Before legislating a new right governing the use" of AI-generated likenesses, Sheffner urged the subcommittee "to first pause and analyze whether the harms it seeks to address are already covered by existing law."

"Often the answer will be 'yes,' indicating that a new law is not necessary," he added.

Calls for quick action

But Warner Music Group CEO Robert Kyncl urged the subcommittee to move quickly on protecting the copyright of artists and other creatives from the use of unauthorized AI-generate replicas.

"The development of AI technology is moving very quickly, and Congress should act now to establish reasonable guardrails which ensure that AI models, digital platforms, artists, songwriters, and other intellectual property owners can prosper together," Kyncl told senators in his testimony.

"As the Committee moves toward the introduction and movement of a Senate bill soon after this hearing, I would like to highlight several elements that we believe any effective bill on deep fakes and voice clones must have to be meaningful," he added, calling for revisions to the draft plan on enforcement and First Amendment protections.

"Legislation must give each person an enforceable intellectual property right to their own individual name, likeness and voice which will allow them to license or authorize use of that property right on free-market terms, deny use of that property right and seek redress in cases of unauthorized use," Kyncl recommended.

He added that online platform companies should not be exempt from those enforcement requirements under section 230 of the 1996 Telecommunications Act, which granted immunity for hosting third-party content with the goal of promoting innovation.

"As this would be an intellectual property right, creators of unauthorized deep fakes should not be shielded by Section 230 of the Communications Decency Act," he told the subcommittee.

"Legislation must acknowledge and respect important First Amendment principles without going further than what the First Amendment protects. The harsh reality is that AI can put words in your mouth. AI can make you say things you didn't say, don't believe, and would never want to be associated with you," according to Kyncl.

"That's not freedom of speech," he asserted.

Additional exclusions

Yet University of San Diego School of Law professor Lisa Ramsey urged the subcommittee to extend exclusions in the draft bill to avoid running afoul of free-speech protections.

"Vague laws are inconsistent with the free speech right because they can have a chilling effect on speech," Ramsey told the subcommittee in her testimony. "Thus, I commend the senators who included specific exclusions from liability for constitutionally protected speech in the No FAKES Act," she said, adding: "Congress should also adopt a safe harbor provision for online service providers willing to implement a notice and takedown system."

Other exclusions offered by Ramsey include the use of AI-generated replicas for educational purposes and the inclusion of a "catch-all" provision to be applied by the courts to allow for fair uses of AI-generated content.

"Another suggestion is to add a 'catch-all' provision at the end of the list of exclusions which explicitly allows courts to limit application of the statute in other ways to protect freedom of expression and other public interests, such as fair competition," Ramsey recommended.

"Congress could add a fair use defense here similar to the copyright fair use defense in Section 107 of the Copyright Act," she added.

The current version of the draft NO FAKES Act includes exclusions for news, public affairs, sports broadcasting and documentaries.

The NO FAKES Act would address the use of non-consensual digital replications of audiovisual works or sound recordings by holding individuals or companies liable if they produce an unauthorized digital; holding platforms liable for hosting an unauthorized digital replica if the platform has knowledge that the replica was not authorized by the individual depicted; and excluding certain digital replicas from coverage based on recognized First Amendment protections, according to a summary of the draft bill.

Other witnesses were SAG-AFTRA national director Duncan Crabtree-Ireland and music artist Tahliah Debrett

Barnett, known as FKA twigs, who both voiced strong support for quick congressional action to protect the rights of content generators.

Digital Media Association president Graham Davies called for "narrowly tailored" legislation that assigns liability to the generator of unauthorized content.

"The primary targets of any future claims brought under a new federal right should be the individuals or organizations that create the violative content," Davies told the subcommittee.

"That is both the most fair approach — liability should rest with the person who intended to cause the harm — and the best way to ensure that only illegitimate content is targeted and removed, because the originator will be in the best position to defend the replica," he added.

California moves bill requiring disclosure of data used to train AI systems

Posted May 2, 2024

California lawmakers are advancing a bill to require AI developers to publicly disclose specific information related to training those systems and services by 2026, despite opposition from major industry and business groups arguing the sweeping proposal would force companies to divulge confidential business information, among other complaints.

"Currently we are seeing neither openness nor accountability from the largest developers of generative AI models, and they are setting the benchmark for everyone else," Rob Eleveld, cofounder and chairman of the Transparency Coalition, testified in favor of the bill, AB 2013, during an April 30 hearing of the state Assembly Privacy and Consumer Protection Committee.

"We are supportive of [this] bill providing clear guidance to the AI developers and owners because all key stakeholders deserve to understand what is being pulled into these models to drive their outputs," Eleveld said about his group, which advocates for transparency around the training of and data used by artificial intelligence models.

The committee approved AB 2013 by Assemblywoman Jacqui Irwin (D) on an 8-1 vote, with two members not voting. It now moves to the Assembly Appropriations Committee for consideration.

A coalition of industry and business groups, including the California Chamber of Commerce and TechNet, is opposed to AB 2013 unless it is amended further, while the Chamber of Progress is opposed outright, according to a committee analysis of the measure.

Specifically, the bill requires "a developer of an AI system or service to post documentation related to its training data to the developer's internet website on or before January 1, 2026, and before each time thereafter than an AI system or service is made available to Californians," the analysis explains.

In addition, AB 2013 requires documentation related to training data to contain a description of each dataset used to develop the AI system or service, including: the source or owner of the dataset; a description of how the dataset furthers the intended purpose of the system or service; the number of data points included in the dataset, with estimated figures for dynamic datasets; and a clear definition of each category associated with data points within the dataset, including the format of data points and sample values.

Other information required by the bill includes: whether the dataset includes any data protected by copyright, trademark, or patent, requiring the purchase or licensure of the data, or whether the dataset is entirely in the public domain; whether the data was purchased or licensed by the developer; whether the dataset includes personal information; whether the dataset includes aggregate consumer information; a description of any cleaning, processing, or modification to the dataset by the developer, including the intended purpose of those efforts; the period during which the data was collected; whether data collection is ongoing; and the dates the dataset was first and last used during development of the AI system or service.

Further, AB 2013 requires the disclosure of whether synthetic data was used to develop AI systems and services.

The bill exempts AI systems or services whose sole purpose is to help ensure security and integrity, the analysis notes.

In response to concerns raised by industry and business groups that the bill requires far too much specific data to be disclosed and could inadvertently expose companies' confidential data, Assemblywoman Irwin agreed to an amendment recommended by the committee.

The amendment requires a "high-level summary" of the datasets used in the development of the system or service, rather than a detailed description of each.

Industry concerns

Ronak Daylami, a policy advocate with the California Chamber of Commerce, thanked Irwin for agreeing to that amendment, but said the chamber and allied groups are still opposed to AB 2013 unless it is further amended. Their concerns "relate to the bill's application to all AI systems and services, not just high-risk ones, and its retroactive application to existing systems and services and not just new ones," she told the committee.

First, "it would be impossible to comply with the mandates of the bill if the business has not maintained the necessary information from when the system or service was first developed years ago," she continued. "And second, just the sheer volume of systems and services implicated by the bill and the level of detail mandated in these disclosures make compliance unmanageable when applied retroactively."

In addition, "Our other major concern relates to the risk posed to trade secrets or other confidential business information — while it may not be obvious on its face, the expertise and judgment as well as the actual selection of data and datasets chosen to train a specific AI model is itself proprietary," she added.

U.S. Chamber seeks more engagement with officials on AI procurement policy

Posted May 1, 2024

The U.S. Chamber of Commerce is urging federal officials to expand the opportunity for industry engagement on the Office of Management and Budget's inquiry into revamping procurement policy to address the benefits and risks of artificial intelligence, in comments that reiterated industry concerns over a short comment deadline under an OMB request for information.

"In conclusion, we appreciate the opportunity to provide high-level feedback on the request for information. The Chamber believes that more time is necessary for stakeholders to review and provide more substantive feedback, as the request will substantially impact the government's ability to take advantage of AI tools," the Chamber said in its comments to OMB.

"We encourage OMB to provide other opportunities to receive input from stakeholders regarding these issues. We are willing and ready to work with OMB and the Office of Federal Procurement Policy to ensure the government's safe and secure use of AI," the Chamber said.

OMB on March 28 finalized guidance for federal agencies on implementation of President Biden's Oct. 30 AI executive order and the following day published the new 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, which closed on April 29, immediately stirred industry concerns.

Submissions from groups including the Information Technology Industry Council and BSA-The Software Alliance urged OMB to rely on "commercial solutions" and both groups said vendor safety assessments can meet the federal government's needs.

The Chamber hit on these issues as well, largely in alignment with the other industry groups, while pressing the case that greater government-industry engagement is necessary before proceeding with highly consequential procurement regulations.

"We remain concerned, however, with the short comment period provided. As we previously shared, the '[s]hort overlapping timelines for agency-required action endangers necessary stakeholder input, thereby creating conditions for ill-informed rulemaking and degrading intra-government cooperation.' Because this request for information provides stakeholders and the business community with only 30 days to comment, we can provide you with only limited feedback and comments," the Chamber said.

Among the key issues that have industry's attention under this RFI, the Chamber calls for specific steps to "promote competition":

- *The federal government must invest in sustained IT modernization, including moving legacy systems into cloud-native environments. This strategic investment provides the foundation for the ecosystem to thrive by ensuring agencies can take advantage of cutting-edge solutions across the vendor community.*
- *Agencies need to inventory and review their data to determine how best to use it strategically for their missions.*
- *Agencies need access to various tools and models to allow for necessary innovation and avoid vendor lockout.*
- *The federal government must ensure the interoperability of systems to promote competition and new entrants while allowing for robust AI security.*
- *OMB should emphasize the importance of access to commercial cloud computing as a platform for AI innovation and IT compliance at scale.*

The Chamber discussed the lines of responsibility between vendors and agencies, saying "differences exist" and arguing that "vendors should be responsible for conducting an assessment to ensure it meets existing safety standards, and the agencies should assess the intended use and application of the system."

On documentation, the Chamber said, "The government should not request any specific training data or data sets on AI models that the government acquires from vendors because: (1) they are impossible for procurement officials to wade through; (2) detailed reviews of the training data will not answer questions about model outputs; and (3) the data sets and their weights are trade secrets and intellectual property that vendors look to protect."

On "notice and appeal," the Chamber said, "We support an appeals process that allows for public engagement when there is an allegation of an unfair result. Without such an ability, the public would be denied the essential capability to protect their rights and allow for the necessary trust in the technology to develop."

"Under such circumstances," the Chamber said, "agencies should engage based on their respective policies. Further-more, an appeal must be explicitly directed at the agency and not the vendor. Agencies have an important role in protecting vendors' intellectual property and property information during an appeal process."

The Chamber framed its comments around its "strong belief" that "public sector utilization of artificial intelligence can improve the efficiency of the federal government and facilitate easier public interaction."

FAA reauthorization bill points to China in calling for report on AI use for safety and efficiency

Posted May 1, 2024

After months of proxy sparring between industry and civil liberties groups, legislation to authorize billions in funding for the Federal Aviation Administration does not ban facial recognition technology for traveler identity verification and would require the head of the agency to report on how airports — possibly including those in China — are using artificial intelligence to improve their operations.

"The [FAA] Administrator shall conduct a review of current and planned artificial intelligence and machine learning technologies to improve airport efficiency and safety," reads text of the giant bill, which reflects a bicameral, bipartisan agreement that would also authorize funding for the National Transportation Safety Board along with a host of other consumer protection and workforce provisions.

Cloture was filed on the bill last week and floor action is expected May 1.

Leading up to the final agreement, announced April 29, trade associations and individuals from the facial recognition technology industry sounded off against efforts to ban its use by the Transportation Security Administration, which in June announced plans to drastically increase its rollout across the country.

"We understand several senators will soon ask conferees on the FAA Reauthorization measure to include in the final agreement an extraneous provision that seeks to prohibit [TSA] from using facial recognition technology (FRT)," reads an April 15 letter the Security Industry Association and the International Biometrics and Identity Association sent to Sens. Maria Cantwell (D-WA) and Ted Cruz (R-TX) and Reps. Sam Graves (R-MO) and Rick Larsen (D-WA).

That provision "would force the agency to abandon its highly successful use of facial biometrics to verify required traveler documents at security checkpoints," the groups wrote. "This 11th-hour measure will compromise programs that facilitate the safety and enhance the travel experience of travelers across the nation."

In November, Sen. Jeff Merkley (D-OR) — joined by Sens. John Kennedy (R-LA), Roger Marshall (R-KS), Elizabeth Warren (D-MA), Edward Markey (D-MA) and Bernie Sanders (I-VT) — introduced the Traveler Privacy Protection Act of 2023, which would "require explicit congressional authorization in order for the TSA to use facial recognition technology in the future; immediately ban the TSA from expanding its pilot facial recognition program; [and] require TSA to end its pilot facial recognition program and dispose of facial biometrics," according to a press release from Kennedy's office.

TSA's plans would broaden use of the technology from a pilot of just under 60 airports to more than 400 over the coming years, according to the agency, with Administrator David Pekoske indicating his intention to eventually require its use across the board.

TSA's growing use of Facial Recognition technology has aligned groups like the American Civil Liberties Union with far-right conservatives like Rep. Jim Jordan (R-OH) in arguing against mirroring countries like China in widescale deployment of the technology.

But in February the *New York Times* quoted former acting Department of Homeland Security Secretary Kevin McAleenan, who is now CEO of travel technology company Pangiam, on why the U.S. is "lagging" behind China in its adoption of the technology.

According to text of the FAA reauthorization bill, in conducting their review, which must be reported to the committees of jurisdiction within a year of the bill's enactment, the administrator "may consider identifying best practices and lessons learned from both domestic and international artificial intelligence and machine learning technology applications to improve airport operations."

The bill would allow the administrator to "[coordinate] with other relevant Federal agencies to identify China's domestic application of artificial intelligence and machine learning technologies relating to airport operations" in reviewing use of the tech in "Jet bridges; Airport service vehicles; airport movement areas; Aircraft taxi; Air traffic control operations; [and] Any other areas the Administrator determines necessary to help improve airport efficiency and safety."

Pekoske, who, along with officials at DHS, where TSA is housed, has touted the technology's accuracy in accordance with testing at the National Institute of Standards and Technology but reportedly refused to share data on the technology's real-world performance with Merkley and the other senators seeking a ban, saying it is "sensitive security information."

Senate Judiciary panel pledges action to protect intellectual property from AI replicas

Posted May 1, 2024

The leaders of a Senate Judiciary subcommittee are pledging to move legislation this year to protect intellectual property from the growing threat of audio and visual replicas generated by artificial intelligence, with Sens. Chris Coons (D-DE) and Thom Tillis (R-NC) planning to introduce a bill in the coming weeks.

The bipartisan bill, the NO FAKES Act, would be the formal introduction of a "discussion" draft unveiled last fall, and would mark a significant step for the Judiciary subcommittee on intellectual property on moving legislation possibly this year, according to Coons and Tillis and other co-sponsors of the upcoming legislation.

The announcement of the upcoming bill was made at an April 30 subcommittee hearing, which Chairman Coons said was scheduled to get feedback from witnesses in the final drafting of the bill for introduction this month.

Since the draft was unveiled in September, Coons said the subcommittee has received "thousands" of suggested revisions which were focused on five areas of concern.

He said those "core technical areas" are whether "we should include a notice and takedown structure similar" to the Digital Millennium Copyright Act, "whether we've struck the right balance with First Amendment exclusions, whether a 70-year post-mortem term should be adjusted" and "whether our bill should have preemptive impact over similar state laws."

Also, feedback on the bill raised questions about creating a process "by which individuals with limited resources and minimal damages can enforce the rights under the law," Coons said.

The upcoming bill is somewhat unique, according to its proponents, because its protections would extend to content regardless of whether it was created for commercial purposes.

Sen. Tillis said, "We've got to make sure that we come up with concrete solutions" that do not "overreach," while stressing the importance of the "need for legislation."

"We have to act, hopefully in this Congress, we can act, which means we have to move very, very quickly, or at a minimum, lay out a baseline that we can pick up when we come back with a new Congress, and get it right," Tillis said.

The draft bill was unveiled by Coons and Tillis in September 2023 along with Sens. Marsha Blackburn (R-TN) and Amy Klobuchar (D-MN), who are members of the subcommittee. Sen. Richard Blumenthal (D-CT) said at the hearing that he plans to join as a co-sponsor when the bill is introduced.

The NO FAKES Act would address the use of non-consensual digital replications of audiovisual works or sound recordings by holding individuals or companies liable if they produce an unauthorized digital; holding platforms liable for hosting an unauthorized digital replica if the platform has knowledge that the replica was not authorized by the individual depicted; and excluding certain digital replicas from coverage based on recognized First Amendment protections, according to a summary of the draft bill.

Witnesses at the hearing all voiced general support for congressional action to address issues raised by AI-generated replicas. However, concerns about regulating free speech were voiced by Motion Picture Association general counsel Ben Sheffner, University of San Diego School of Law professor Lisa Ramsey, and Digital Media Association president Graham Davies.

Warner Music Group CEO Robert Kyncl, SAG-AFTRA national director Duncan Crabtree-Ireland and music artist Tahliah Debrett Barnett, known as FKA twigs, voiced strong support for quick congressional action to protect the rights of content generators.

Action on industry-backed AI innovation bill delayed as FAA reauthorization advances

Posted May 1, 2024

Just as a major industry group offered praise for the Future of AI Innovation Act, the Senate Commerce Committee has removed the bill — and all other legislation — from the agenda for its May 1 executive session.

"The Future of AI Innovation Act is a refreshing example of how policymakers can and should steer AI toward positive outcomes," Hodan Omaar, senior policy manager for the Center for Data Innovation, wrote in an April 30 press release anticipating the markup. "The bill doesn't just dangle a carrot of progress, it paves a path forward for achieving it."

But according to a late release April 30 from the Senate Commerce Committee, in preparation for legislation to reauthorize the Federal Aviation Administration coming to the floor at the same time, the panel will now only consider nominations during the session.

The committee's release said "the bills originally set to be considered at the markup will be considered at a later date."

"The Act positions the United States to uncover new groundbreaking research and use AI to solve grand challenges," CDI's Omaar said of S. 4178 — the Future of AI Innovation Act. "It unlocks valuable public data needed to fuel AI innovation, it sets up safety mechanisms to better understand what AI systems should and shouldn't be used for, and it fosters international collaboration to catalyze advancements that benefit society as a whole."

The committee's markup agenda had also included the popular CREATE AI Act, S. 2714.

Among other things, S. 4178 would provide a way around provisions in S. 2714 that would limit access to AI resources — including curated public data sets — to academic, non-profit and small business users for public-interest goals by making such data available to "companies of all sizes."

Tech sector leader backs AI vendor testing, commercial product solutions in comments to OMB

Posted May 1, 2024

The Information Technology Industry Council says "commercial solutions" and vendor safety assessments can meet the federal government's needs in purchasing artificial intelligence technologies, in response to the Office of Management and Budget's request for information on possible changes to procurement policy under the Biden administration's AI executive order.

Among OMB's questions in a March 29 RFI, the White House agency asked, "Which elements of testing, evaluation, and impact assessments are best conducted by the vendor, and which responsibilities should remain with the agencies?"

ITI said in its comments, "Vendors who develop AI technology are familiar with existing standards and use these benchmarks to create safe and responsible technologies. Meanwhile, agencies who deploy AI technology are most familiar with their intended uses of specific technologies."

ITI said "vendors should be responsible for conducting assessments that ensure technologies satisfy existing standards, while agencies should be responsible for conducting assessments to ensure that their deployment in a particular circumstance is appropriate."

Further, the group said, "Agencies may also wish to verify vendor assessments against existing standards and frameworks. This approach allocates responsibility according to which actor is in the best position to control each facet (i.e., development vs. deployment) so assessments are performed more effectively."

OMB on March 28 finalized guidance for federal agencies on implementation of President Biden's Oct. 30 AI executive order and the following day published the new request for feedback on how it should apply the EO's provisions on responsible federal procurement of the technology.

A 30-day comment period on the RFI closed on April 29. The request divided ten specific questions into two categories: "Strengthening the AI Marketplace" and "Managing the Performance and Risks of AI."

As in ITI's submission, BSA—the Software Alliance in its OMB submission said, "The Government should rely on commercial solutions to the maximum extent practicable. The [Federal Acquisition Regulation] requires agencies to prioritize commercial solutions over custom-built alternatives."

BSA cited the FAR provisions in arguing that agencies should default to using commercial services instead of developing their own AI systems, and that testing the vendors already conduct on such commercial products and services to provide "quality assurance" should be sufficient.

BSA's comments referenced part 12 of the FAR and ITI also cited that part, with the latter group saying, "It should also be noted that the benefit of leveraging commercial AI is that contract quality assurance is based on the 'contractor's existing quality assurance systems as a substitute for Government inspection and testing before tender for acceptance unless customer market practices for the commercial product being acquired include in-process inspection.' (See FAR 12.208). In this sense, the marketplace already using the product is a useful metric for quality assurance and is part of the quality assurance effort."

That part of the FAR rules reads, "Contracts for commercial products shall rely on contractors' existing quality assurance systems as a substitute for Government inspection and testing before tender for acceptance unless customary market practices for the commercial product being acquired include in-process inspection. Any in-process inspection by the Government shall be conducted in a manner consistent with commercial practice. The Government shall rely on the contractor to accomplish all inspection and testing needed to ensure that commercial services acquired conform to contract requirements before they are tendered to the Government."

In addition, ITI in its comments argued that "transparency around possible assessments … will promote competition and innovation" and noted ongoing work to develop "the science of evaluations," saying "it is premature … to standardize assessments at this time."

The group points to work at the NIST AI Safety Institute Consortium "to research and develop science-based and empirically backed AI guidelines and standards. … We encourage OMB to leverage AISIC's work, which is being supported by more than 200 organizations, including ITI."

Overall, ITI said: "The federal government can strongly benefit from leveraging commercial AI solutions, ideally under the same or substantially similar terms and conditions as those offered to commercial customers. We encourage the government to limit the addition of government-unique terms and conditions to commercial solutions, as doing so drives up the cost and potentially limits the government's access to cutting-edge technologies on par with the commercial marketplace."

ITI said, "We especially urge OMB to require federal agencies to act with caution when modifying commercial terms and conditions related to government rights in data and expansion of liability for suppliers. ITI believes OMB can play a significant role in working with industry to review existing common terms and conditions for IT contracts and ensure that future solicitations prioritize commercial terms and conditions, rather than overly restrictive government-unique requirements."

ITI emphasized, "The government already has all the tools that it needs to buy commercial technology, including policies and procedures for acquiring commercial products and services outlined in FAR Part 12 through FAR Part 15. AI does not need a separate method of procurement and should be treated like any other good or service that the government is purchasing. It is important to note that AI is simply one type of emerging technology."

The tech industry group said, "If OMB's goal is to foster innovation and competition in the federal marketplace, contracts should refrain from specifying the type of technology that must be used and should focus on the desired outcomes and/or deliverables that best fit the desired end goals of the mission."

"In general," ITI said, "as a guiding principle, the procurement process should rely on existing standards and best practices wherever possible and appropriate, including the National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF) and International Organization for Standardization (ISO) standards."

Further, ITI said, "Agencies should focus on use-case-specific governance practices with respect to risk. There should not be a one-size-fits-all assessment framework given the complexity of the different levels of the tech stack where AI may be leveraged."

Presidential advisors eye AI 'field testing' recommendations for law enforcement

Posted May 1, 2024

The National AI Advisory Committee is slated to consider a proposal for "field testing" artificial intelligence technologies for use by law enforcement agencies, with the goal of inclusion in federal guidance under Biden's AI order consistent with the National Institute of Standards and Technology's risk management framework for AI technologies.

"The responsible use of AI in law enforcement requires AI developers to train, test, and audit their AI tools to ensure that the results of a predictive tool are sufficiently accurate, non-discriminatory, rights- respecting, and cost-effective," says a draft recommendations document for the NAIAC to consider for approval at its May 2 public meeting.

The recommendations developed by the NAIAC's law enforcement subcommittee offer a "checklist" for agencies to follow before employing AI-powered tools. The document also includes three recommendations for committee consideration on funding, including whether Congress should enact a "special-purpose grants" program for conducting independent testing of AI law enforcement tools.

The recommendations were approved for consideration by the full committee at an April 16 public meeting of the law enforcement subcommittee.

The proposal is being offered for insertion to White House Office of Management and Budget guidelines issued on March 28 to implement Biden's AI executive order signed on Oct. 30.

"The White House now requires all federal agencies to test an AI tool for performance in real-world settings," says the NAIAC proposal referencing the OMB guidelines.

"Very few resources are available to help guide the AI industry, law enforcement departments, and independent researchers through the process of testing AI tools when they are provisionally used in the field," the NAIAC plan says in laying out the reasons for the recommendations.

The recommendations "provide the infrastructure for AI field testing in the context of policing," it says.

Among its three recommendations, the document offers two options for funding field testing of AI law enforcement tools by state and local authorities.

Option one is the congressionally created fund to be overseen by the Justice Department's Bureau of Justice Assistance, with requests for funding to be reviewed and awarded "based in part on consistency with the Field Test Checklist," the document says.

The second option would be for the White House to "charge NIST and the Bureau of Justice Assistance to create incentives and infrastructure for coordinated field studies of law enforcement tools."

That program "should allow AI companies to propose, and law enforcement agencies to opt into, multi-site field test consistent with the Field Test Checklist" laid out in the document.

"Selected proposals should be supported through equipment purchases, law enforcement grants, IT supports, and research team funding," the document says.

"As with performance, the ultimate goal of guarding against AI bias is to ensure that the community as a whole can have confidence that new policing tools improve equity and fairness rather than exacerbating existing disparities," the document says among its "macro metrics" for testing AI tools.

The NAIAC is also slated to consider a proposal by the law enforcement subcommittee to require public reporting of "high-risk" uses of AI technologies by law enforcement agencies.

"Office of Management and Budget (OMB) — or another appropriate arm of the Executive branch — should require that law enforcement agencies create and publish annual summary usage reports for safety- or rights-impacting AI to be included in the AI Use Case Inventory," the recommendation says.

"Providing a breakdown of use of safety- or rights- impacting AI tools based on case type or other relevant category balances the need for operational security and confidentiality with a level of granularity that allows the public to assess the impact of these systems and agency adherence to their policies," the proposal says.

The proposal builds on the existing Uniform Crime Reporting Program's National Incident-Based Reporting System to "help streamline the administrative burden of additional reporting and encourage consistency across agency reports."

The NAIAC is also slated to consider recommendations on procurement, harnessing AI impacts for science and medicine, and the creation of statewide repositories for body-worn cameras.

NAIAC was created by the National AI Initiative Act of 2020 to advise the president and the National AI Initiative Office in the White House Office of Science and Technology Policy, according to the National Institute of Standards and Technology, which facilitates the advisory group. The committee consists of 26 experts on AI from industry, academia and other research groups. It held its first meeting in May 2022 and issued its first report in May 2023.