INSIDE AI POLICY

Exclusive news on the burgeoning debate over regulating artificial intelligence

Vol. 2, No. 21 — May 21, 2024

Schumer expects AI 'roadmap' to influence House, set long-term trajectory for Congress

Posted May 16, 2024

Senate Majority Leader Charles Schumer (D-NY) plans to meet with House Speaker Mike Johnson (R-LA) to coordinate bicameral efforts on legislating safeguards for artificial intelligence, based on a policy "roadmap" released by Schumer and his bipartisan AI working group led by Sens. Mike Rounds (R-SD), Todd Young (R-IN) and Martin Heinrich (D-NM).

"So, I plan to meet with Speaker Johnson in the very near future to see how we can make this bipartisan effort bicameral," Schumer told reporters May 15 to lay out next steps following the release of the roadmap report.

"And we've talked a little bit about it here and there. And I think he's very interested in doing that. Because after all, this is not and should not be a partisan issue," Schumer added.

Johnson's office did not respond to a request for comment, but Johnson did create an AI task force with Minority Leader Hakeem Jeffries (D-NY) in February. The House task force is led by Reps. Jay Obernolte (R-CA) and Ted Lieu (D-CA).

Schumer's AI working group released its long-awaited report on May 15 to summarize a series of closed-door meetings in the Senate with industry and other AI policy stakeholders last fall and winter with the intention of guiding the chamber's committees in drafting legislation on areas of concern and consensus identified by those talks.

Schumer said the groundbreaking report will set a path for how congressional committees will be able to legislate on the transformational technology which is expected to affect all sectors of the economy.

"This is complex. It affects every area of society and, frankly, Congress doesn't have a roadmap here," Schumer told reporters.

"You know, if it's defense or health, we have committees that have great expertise in those areas and lots of experience. We don't have that here," he added, to note that the report offers guidance for committees in the long-term on traversing cross-cutting issues related to the development and deployment of AI.

"Bottom line, Congress can't and won't solve every challenge AI presents today," Schumer told reporters. "But we can lay down a base of smart bipartisan policy proposals, guided by both urgency and humility, and we can do so this Congress."

"It's my responsibility as leader to lead cross-committee efforts in developing, passing [and] advancing AI legislation in the 118th Congress, and that's what I'm going to do," he added.

Schumer said the report stresses "urgency, humility and bipartisanship" for writing legislation to promote the benefits and minimize the risks of AI.

Sen. Rounds said the report offers a plan for regulating AI in a way that incentivizes the development of AI technologies in the United States.

"Furthermore, with regard to guidelines for regulatory approaches, we understand that if we approach this with really strict guidelines and really strict rules, we may very well chase some of that development outside to other areas, not just in China or in Russia, but in other parts of the world that are inviting them to come in," Rounds warned.

"We want them to feel comfortable being here, while at the same time creating a regulatory environment that incentivizes their development here," he said about AI developers.

Sen. Young stressed that the roadmap calls on committees to consider whether existing laws can be adapted or

continued on next page

In This Issue . . .

expanded to address the issues raised by the emergence of AI technologies.

"With this roadmap, we have provided direction to the committees of jurisdiction so they in a bipartisan fashion can consider legislation, some of which we endorse in the roadmap, most of which will be produced in the coming weeks, months and years by our colleagues," Young told reporters.

To reap the potential benefits and minimize the risks of AI, Young said "we need to make sure that we're taking seriously and learning as much as we can about the perceived and real risks associated with this technology."

"Those will either need to be overcome through innovation itself, or by adapting our existing laws to an AI-enabled world," he said, adding: "If those laws prove unfit for the purpose of mitigating against potential risks, then they'll need to be amended in various ways."

Sen. Heinrich said "what we've done with this roadmap is really just mapped out for the committees, that we've never wanted to supplant or circumvent, where some of the areas of relative consensus that are ripe for bipartisan action today."

He said "things like investment in research and development, and the necessity of that for us to maintain our competitiveness . . . [and] democratizing some of that research and development," are core goals of the roadmap report.

Heinrich made a pitch for the CREATE AI Act which would authorize and fully fund the National AI Research Resource, a Biden administration pilot project for expanding access to the computational resources needed to develop AI beyond big companies. The bill was introduced by all three members of Schumer's AI working group, and Heinrich noted that the Commerce Committee is slated to soon mark up the bipartisan bill.

Schumer noted that the report proposes spending $32 billion over the next several years as a starting point to boost those research efforts. And Rounds cited the upcoming annual National Defense Authorization Act as an opportunity for moving AI-related legislation this year.

"Just to follow up on that, just as an example, the NDAA passes every single year, bipartisan in nature, and we try to do our best to keep it as much defense focused as possible," Rounds said.

"But in defense, we need additional resources with regard to the development of AI within our weapons systems, but also, so that we can be more efficient in our depot operations and in our acquisitions processes," he added.

"The sooner we incorporate AI into those, the better off we're all going to be, and the money that we can save will actually be realized by taxpayers in the long term," Rounds said.

Schumer's AI 'roadmap' details national security priorities as NDAA debate begins

Posted May 21, 2024

Senate Majority Leader Charles Schumer's (D-NY) recently released "roadmap" for artificial intelligence policies addresses priorities for protecting national security, including countering China's growing influence and the need for increased staff training at the Defense Department, just as lawmakers are gearing up to debate the fiscal 2025 National Defense Authorization Act.

"In order to ensure that our adversaries don't write the rules of the road for AI, participants reinforced the need to ensure the DOD has sufficient access to AI capabilities and takes full advantage of its potential," says the roadmap released May 15 by Schumer and his bipartisan AI working group led by Sens. Mike Rounds (R-SD), Todd Young (R-IN) and Martin Heinrich (D-NM).

The highly anticipated roadmap report was issued to summarize a series of closed-door meetings hosted by Schumer and the working group last fall and winter with leaders from industry, labor, the civil rights movement and academia, among others, to identify areas of consensus for legislating AI safeguards.

National security was a theme at one of the meetings and Sen. Rounds has said that the proposals offered there and outlined in the report are intended to inform the committee process for drafting the next annual NDAA. Rounds is a senior member of the Senate Armed Services Committee and ranking member of its cybersecurity subcommittee.

The Senate Armed Service Committee is slated to begin its markup of the fiscal 2025 NDAA on June 12, while the

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.

House Armed Services Committee announced this week that its markup will begin May 22.

"To maintain a competitive edge, participants agreed that it would require robust investments from the U.S. in AI research, development, and deployment," says the Senate roadmap report about discussions at the national security meeting last year.

"From gaining intelligence insights to supercharging cyber capabilities and maximizing the efficiency of drones and fighter jets, participants highlighted how the U.S. can foster innovation in AI within our defense industrial base," the report adds.

"Participants raised awareness about countries like China that are heavily investing in commercial AI and aggressively pursuing advances in AI capacity and resources," the report says.

Countering China has been a rallying point for many congressional proposals on regulating and promoting AI uses, and the Schumer report appears to indicate the NDAA will be a significant legislative vehicle for advancing counter-China measures related to AI this year.

"The AI Working Group will collaborate with committees and relevant executive branch agencies to stay informed about the research areas and capabilities of U.S. adversaries," the roadmap report says.

"Managing talent in the realm of advanced technologies presents significant challenges for the DOD and the Intelligence Community (IC)," the report adds.

To address those concerns, Schumer and his group encourages DOD and the IC "to further develop career pathways and training programs for digital engineering," the report says. And specially for AI training, the group is calling on the committees to fully implement section 230 of the fiscal 2020 NDAA.

Section 230 directed DOD "promote and maintain digital expertise and software development as core competencies" for both its military and civilian workforces.

The fiscal 2020 NDAA also called on the Pentagon to establish the Chief Digital Engineering Recruitment and Management Office. The AI roadmap is urging additional support for that office.

"Supports the allocation of suitable resources and oversight to maintain a strong digital workforce within the armed services," says the roadmap report among its policy priorities for national security.

"Urges the relevant committees to maintain their efforts in overseeing the executive branch's efficient handling of security clearance applications, particularly emphasizing swift processing for AI talent, to prevent any backlogs or procedural delays," is another recommendation by the Schumer report.

And it encourages "relevant committees to develop legislation to improve lateral and senior placement opportunities and other mechanisms to improve and expand the AI talent pathway into the military."

The Schumer group also weighs in on the highly controversial use of AI for lethal autonomous weapons systems such as drones, arguing that transparency around the use of such systems will be crucial.

"The AI Working Group recognizes the DOD's transparency regarding its policy on fully autonomous lethal weapon systems," the report says.

"The AI Working Group encourages relevant committees to assess whether aspects of the DOD's policy should be codified or if other measures, such as notifications concerning the development and deployment of such weapon systems, are necessary."

Also, Schumer's AI group is encouraging the White House "Office of the Director of National Intelligence, DOD, and [the Department of Energy] to work with commercial AI developers to prevent large language models, and other frontier AI models, from inadvertently leaking or reconstructing sensitive or classified information."

The House Armed Services Committee in preparation for marking up its fiscal 2025 NDAA later this week has released draft proposals that already include some AI-related provisions.

For instance, a draft "chairman's mark" of the bill includes provisions requiring the Pentagon to audit and report its spending on AI technologies.

"The committee is concerned about accurate budgeting for inclusion" of AI, machine learning and computer vision into Pentagon programs, says the May 13 draft legislative proposal.

"Therefore, the committee directs the Secretary of Defense, in coordination with the Undersecretary of Defense for Acquisition and Sustainment, to report to the House Committee on Armed Services by March 1, 2025, with a plan to ensure the budgeting process for programs containing AI elements such as ML and CV, include estimates for the data required to train, maintain and improve AI models or systems," the bill says.

A separate draft plan released by the Armed Services cyber, IT and innovation subcommittee includes provisions for DOD to develop a strategy on preparing the massive amounts of data generated by the military for use by AI technologies, with a focus on encouraging seamless integration across military operations.

The data management strategy required of the Secretary of Defense within 270 days must include the "activities of the Chief Digital and Artificial Intelligence Officer of the Department of Defense to increase and synchronize the use of modern data formats and modern data sharing standards across the Department of Defense, including the Armed Forces in the Department of Defense," according to the section on "usability of antiquated data" in the subcommittee draft bill.

The Senate Armed Services Committee has not yet released any draft proposals for its June 12 markup.

Group chaired by former USPTO directors questions office's AI guidance over 'human contribution'

Posted May 21, 2024

The Council for Innovation Promotion, a group co-chaired by former U.S. Patent Office directors, says draft USPTO guidance on artificial intelligence would inject uncertainty into the process of obtaining patent protection for inventors using AI, and urges that the document be withdrawn or substantially rewritten.

"C4IP is concerned that the Office's artificial intelligence (AI) inventorship guidance will ultimately hurt humans, human creativity, and flourishment; the very opposite of what the Office set out to do," the group says in comments to USPTO.

"The newly announced guidance means that inventors who use artificial intelligence to innovate and then seek patent protection will be faced with uncertainty throughout the examination process and during any validity challenges afterward, with the possibility that their 'human' contribution was not enough," C4IP says.

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

The guidance, on the question of patentability, says, "While AI systems and other non-natural persons cannot be listed as inventors on patent applications or patents, the use of an AI system by a natural person(s) does not preclude a natural person(s) from qualifying as an inventor (or joint inventors) if the natural person(s) significantly contributed to the claimed invention, as explained in section IV of this notice."

It says, "Patent applications and patents for AI-assisted inventions must name the natural person(s) who significantly contributed to the invention as the inventor or joint inventors (i.e., meeting the *Pannu* factors as explained in section IV). Additionally, applications and patents must not list any entity that is not a natural person as an inventor or joint inventor, even if an AI system may have been instrumental in the creation of the claimed invention. This position is supported by the statutes, court decisions, and numerous policy considerations."

The C4IP submission was signed by executive director Frank Cullen, a former vice president at the U.S. Chamber of Commerce.

The group's board of directors is co-chaired by Andrei Iancu, who was USPTO director during the Trump administration, and David Kappos, USPTO director during the Obama administration.

"C4IP is a bipartisan coalition dedicated to promoting strong and effective intellectual property rights that drive innovation, boost economic competitiveness, and improve lives everywhere," the group says. "Founded and chaired by former directors of the U.S. Patent and Trademark Office from previous Democratic and Republican administrations, our nonprofit organization aims to be a valued partner to those considering policies impacting America's IP system."

The trouble with the USPTO guidance on AI, C4IP says in its comments to the patent office, is that it "starts from the premise that use of AI by an inventor or inventors is different than the use of any other tool. This premise is simply incorrect. To date, the possibility that AI can act as an inventor, absent any human involvement, remains a hypothetical, not an issue that warrants a significant overhaul of existing rules, as the Office proposes to do here — indeed, all the examples crafted by the Office describe varying degrees of human involvement."

"Yet," C4IP says, "under the guidance's reinterpretation of case law on conception and inventorship, no one will be entitled to a patent where no human made a 'significant contribution' to the conception of the invention. But this test was developed to answer a different question — namely, to decide who invented something first or whether someone was improperly listed or omitted as an inventor."

C4IP says, "It is in this context that the significance (or lack thereof) of particular contributions becomes relevant."

According to the group, "The context of a human or humans using AI is fundamentally different. The proper analytic framework for considering use of AI should be the same as what patent law has always used to consider tools or other input used by inventors. The law here is clear, as set forth in the last line of § 103: 'Patentability shall not be negated by the manner in which the invention was made.'"

C4IP says, "Inventors' use of AI merits no further consideration in the patentability analysis than the use of any other tool, such as a computer, for example, under fact patterns more analogous than those considered by the Office. This is because the Office is properly considering 'how' the invention is made, not 'who' the inventors are."

It says, "Ensuring a robust and reliable patent system in the face of ongoing technological advancement is a crucial component of the USPTO's mission. Yet, missteps in accommodating such development can have unintended but substantial chilling effects on further progress. C4IP believes this guidance on AI and inventorship, by effectively assuming too much about AI and too little about humans, has the potential to do just that."

"The solution," according to C4IP, "is fortunately simple: treat AI just as patent law has treated other new tools and allow relevant case law to be developed by the courts or for Congress to act. Until then, C4IP respectfully suggests that the USPTO consider rescinding or substantially revising this guidance."

Colorado Gov. Polis signs AI bill to inform national debate, while calling for federal law

Posted May 21, 2024

Colorado Gov. Jared Polis (D) has signed legislation "concerning consumer protections in interactions with artificial intelligence systems," hailed as the first of its kind in the country, while asserting the need for federal legislation that would govern all states.

"Should the federal government not preempt this with a needed cohesive federal approach," Polis said in a May 17 signing statement, "I encourage the General Assembly to work closely with stakeholders to craft future legislation for my signature that will amend this bill to conform with evidence-based findings and recommendations for the regulation of this industry."

State and federal Democrats' position on the preemption issue in the privacy and data security arena has typically been represented by fierce defense of state laws amid the potential for a weaker national standard. But in the case of Colorado's SB 24-205, there are concerns about how the bill will affect both industry and consumers, with opponents highlighting its "horrendous" loopholes.

With the bill not set to take effect until February 2026, and state procedure allowing for its revision before then, consumer advocates have supported the governor signing it while noting the importance of creating a path for regulating AI systems such as those that can determine who gets hired for a job or approved for a loan.

The Colorado bill would require developers and deployers of high-risk artificial intelligence systems to use reasonable care to avoid algorithmic discrimination. It provides a "rebuttable presumption" that such care was used if the entities developing and deploying such systems comply with provisions outlined in the legislation as well as rules to be issued by the state Attorney General.

Chief among those provisions, deployers must complete annual impact assessments of their systems and disclose any related discoveries to the Attorney General within 90 days. Accordingly, developers of such systems must make summaries of their training data and other documents deemed necessary to conduct those impact assessments available to the deployers. Developers must also similarly report any "known or reasonably foreseeable risk of algorithmic discrimination" to the Attorney General within 90 days of their discovery.

The Attorney General's rulemaking would lay out the specifics of the necessary impact assessments and other key provisions of the legislation. However, the bill itself defines what qualifies as a "high risk" AI system, and consumer advocates are concerned some of those definitions could undermine its stated goal.

"Consumer Reports believes that this law makes an important step forward, but it does not go far enough to protect consumers from biased AI systems," the group said in a May 18 release. "There are several loopholes that ought to be closed and provisions that must be updated over the course of Colorado's next legislative session."

"For example, the bill exempts AI technology that performs 'narrow procedural task[s]' from its definition of high-risk AI," the release notes. "This term is undefined, and companies may argue that all manner of high-stakes decisions — screening out resumes, scoring college applicants — are 'narrow procedural tasks.'"

While noting his "reservations" in signing the bill, Polis said, "this is an important conversation to have, and in signing this bill I hope that it furthers the conversation, especially at the national level."

California legislature's fiscal committees advance host of AI policy, regulatory bills

Posted May 21, 2024

Appropriations committees in the California legislature are advancing a host of AI policy and regulatory bills, including several high-profile measures opposed by major industry organizations that generally argue they place overly broad and stringent new rules on the sector.

Many of the bills were cleared by fiscal committees by a May 17 deadline, teeing them up for imminent floor votes in California's Senate and Assembly. May 24 is the deadline for each house to pass bills introduced in their chamber.

One of the most controversial bills, SB 1047 by Sen. Scott Wiener (D), was approved by the Senate Appropriations Committee May 16 on a 5-0 vote with two Republican senators choosing not to vote.

SB 1047, the Safe and Secure Innovation for Frontier Artificial Intelligence Systems Act, would establish sweeping regulations to govern the largest and most powerful artificial intelligence systems. The bill is opposed by major industry players and there remain numerous unresolved questions and concerns which are expected to be addressed in the coming weeks as the bill moves through the legislative process.

The legislation "requires developers of powerful artificial intelligence models and those providing the computing power to train such models to put appropriate safeguards and policies into place to prevent critical harms," explains a recent committee analysis. "The bill establishes a state entity to oversee the development of these models and calls for

the creation of a public cloud computing cluster."

Another high-profile bill that is opposed by industry is SB 942, which "places obligations on businesses that provide generative artificial intelligence (AI) systems to develop and make accessible tools to detect whether specified content was generated by those systems," according to a Senate floor analysis. These "'covered providers' are required to include visible and imperceptible markings on AI-generated content to identify it as such."

In response to industry opposition, SB 942 was amended May 16 in the Senate Appropriations Committee to delete a section creating a "Generative AI Registry Fund" and requiring a covered provider to register with the Department of Technology and provide to the department a URL to any AI detection tool it has created. Also stricken from the bill was a provision authorizing the department to charge a registration fee on covered providers.

Nevertheless, an industry coalition being led by TechNet argues in opposition to SB 942 that the bill "enacts requirements for a technology that is still under development and rapidly evolving," the analysis states, quoting a letter from the group. "For example, there isn't a program that can watermark text, making the bill's requirements to do so impossible to comply with. We believe references to text watermarking should be removed to reflect this reality."

The Senate Appropriations Committee also passed several bills — SB 896, SB 892 and SB 893 — aiming to establish first-time accountability and safety standards for AI technologies, including a measure that codifies into state law President Biden's AI Bill of Rights and establishes the legislature's intent that the private sector adhere to AI safeguards and protections.

Other key bills

Other significant fiscal and non-fiscal AI bills advancing last week in the California legislature include:

- AB 2013, which requires a developer of an AI system or service to publicly disclose specific information related to the system or service's training data.
- AB 1791, which requires social media platforms to delete provenance data related to a user's identity from content uploaded to the platform, while retaining provenance data related to the system or service used to generate the content, according to an Assembly floor analysis.
- AB 1836, which establishes a specific cause of action for beneficiaries of deceased "personalities" — individuals whose likeness has commercial value at the time of their death — for the unauthorized use of a digital replica of the celebrity in audiovisual works or sound recordings, states an Assembly floor analysis.
- AB 2355, which requires certain political advertisements to include a disclosure that the advertisement was generated or substantially altered using AI.
- AB 2839, which prohibits the distribution of an advertisement or other election communication containing certain materially deceptive and digitally modified or created content with the intent to influence an election or solicit campaign funds, according to an Assembly Appropriations Committee analysis.
- AB 2930, which implements a regulatory framework for use of automated decision tools (ADTs), with the goal of preventing algorithmic discrimination, and authorizes the Civil Rights Department and specified public prosecutors to enforce violations, an Assembly Appropriations Committee states.

Meanwhile, the Assembly Appropriations Committee declined to advance two AI-related bills by not bringing them up for a vote.

They are AB 2652, which would have required the Superintendent of Public Instruction to convene a workgroup related to AI in educational settings; and AB 3204, which would have established a "data digester" registry, overseen by the California Privacy Protection Agency, that collects and provides to the public information about entities that use personal information to train AI systems, according to analyses by the panel.

House Homeland Security sets witnesses for hearing on AI and cybersecurity

Posted May 20, 2024

The House Homeland Security Committee will examine cybersecurity implications of artificial intelligence and the role of AI in "homeland security missions" at a May 22 hearing featuring witnesses from technology, security and digital rights groups, the committee has announced.

The committee on May 20 named four witnesses for the session: Troy Demmer, co-founder and Chief Product Officer at Gecko Robotics; Michael Sikorski, CTO and VP of engineering at Palo Alto Networks; Ajay Amlani, president and head of the Americas at iProov; and Jake Laperruque, deputy director of the Security and Surveillance Project at the Center for Democracy and Technology.

House Homeland Security Chairman Mark Green (R-TN) announced the hearing in a May 18 statement, saying, "Artificial intelligence is not only revolutionizing the productivity and efficacy of our industry sectors, but it has the potential to be a turning point for the homeland security mission."

Green said, "I look forward to examining ways AI can fill workforce gaps, enhance our collective cyber defense,

and spur innovation in a way the American people can trust."

Green and Homeland Security ranking member Bennie Thompson (D-MS) had invited Microsoft vice chair and president Brad Smith to testify at a May 22 session on a recent Cyber Safety Review Board report that sharply criticized the company over the 2023 Microsoft Exchange Online cyber intrusion. But Microsoft declined to make Smith available this week, according to a committee source, and the panel decided to move ahead with an AI hearing.

The House Homeland Security Committee's cyber panel held a hearing in December on DHS' role in implementing President Biden's Oct. 30 executive order on artificial intelligence.

OpenAI argues burden of multiple lawsuits hinders ability to meet over document dispute

Posted May 20, 2024

OpenAI is telling a federal district court that the resource burden of multiple copyright infringement lawsuits filed over the training of its ChatGPT generative artificial intelligence model prevents the company from being able to periodically meet with class-action plaintiffs over their request for company documents.

"OpenAI is currently a defendant in seven copyright-based lawsuits with overlapping facts, claims, issues, and defenses," say lawyers for defendant OpenAI in a May 17 letter to the U.S. district court for southern New York.

"No party appears to dispute there is significant (although not complete) overlap, or that coordination of discovery is necessary. Indeed, Plaintiffs themselves have called for coordination since this lawsuit's earliest days," the letter says.

But OpenAI tells the court that the plaintiffs' request for biweekly meetings to resolve a simmering dispute over access to company documents is excessive and overly burdensome.

"OpenAI agrees that a case management conference is warranted, particularly given Plaintiffs' ongoing refusal to participate in the coordination of discovery among several related cases notwithstanding Plaintiffs' own previous requests for such coordination," the company's lawyers write in their letter to the court.

"OpenAI disagrees that bi-weekly discovery conferences and briefing are necessary or an efficient use of judicial resources, and disputes Plaintiffs' misleading characterization of the parties' discovery efforts to-date."

OpenAI's letter is the latest development in *Authors Guild et al. v. OpenAI et al.* over access to documents during the discovery phase of the lawsuit.

The dispute underscores how important information about how AI developers train their generative models has become among the various copyright infringement cases recently filed against the industry.

Plaintiffs in *Authors Guild* have raised concerns with the court that defendants appear to be trying to run out the clock in an attempt to deny or limit access to the requested information.

"With just four months remaining before the discovery cutoff, and less than a month before the June 14, 2024 substantial completion deadline, the Court's intervention is necessary to hold all parties accountable to the current schedule," said a May 15 letter to the court by plaintiffs that proposed the disputed biweekly meetings.

But OpenAI argues that plaintiffs have "stonewalled any attempt at coordination" on discovery.

"Meanwhile, without acknowledging OpenAI's May 7 email [requesting coordination], the Plaintiffs in this case and *In re ChatGPT* have made separate requests for depositions requiring the same witness to testify, underscoring the need for coordination," the company argues.

"Instead, Plaintiffs have rushed to this Court to demand unnecessary and burdensome procedures in a letter that mischaracterizes the state of discovery and meet-and-confers," the letter says.

"First, Plaintiffs have not identified a single outstanding discovery issue that currently requires use of the Court's limited resources, let alone a multitude of issues that would warrant the overbroad Court oversight," according to the letter.

"Second, bi-weekly status updates and discovery conferences will add unnecessary complexity and burden to this already truncated case schedule." And third, "none of Plaintiffs' cited cases even addressed bi-weekly discovery conferences. Moreover, the cases are inapposite," the company argues while citing past magistrate rulings as precedent.

At the same time, defendant Microsoft is arguing that the request by plaintiffs for biweekly meetings would prove "to be unnecessary and inefficient," in a separate May 17 letter to the court.

Microsoft was cited as a defendant in the *Authors Guild* and other copyright infringement cases because of its financial support for OpenAI's research on its generative AI models.

"Microsoft has not missed any deadlines, has not refused to work with Plaintiffs, and has not caused any delay to the agreed case schedule," the company tells the court.

But Microsoft argues the plaintiffs' proposal for regular meetings on requested documents that they say will prove the companies violated copyright protections is excessive.

"Far from being a 'tried and true' measure made necessary by Plaintiffs' litany of complaints about discovery, the bi-weekly conferences requested by Plaintiffs are a dramatic intervention reserved for extreme circumstances plainly not present here," the Microsoft letter argues.

Schumer's release of AI 'roadmap' shifts focus to Senate committees drafting and moving legislation

Posted May 20, 2024

Senate Majority Leader Charles Schumer's (D-NY) release of a "roadmap" report on AI policies shifts the focus, and burden, to the various committees on drafting legislation to promote the benefits and mitigate the risks of artificial intelligence.

The highly anticipated report concludes a major chapter in the Senate's efforts to harness the transformative power of AI and launches what could be an uncertain and contentious committee process.

"From the outset, the AI Working Group's objective has been to complement the traditional congressional committee-driven policy process," says the May 15 report released by Schumer and his bipartisan AI working group led by Sens. Mike Rounds (R-SD), Todd Young (R-IN) and Martin Heinrich (D-NM).

"Given the cross-jurisdictional nature of AI policy issues, we encourage committees to continue to collaborate closely and frequently on AI legislation as well as agree on shared clear definitions for all key terms," the report says while suggesting the challenges committee leaders may face in wrangling what even the working group agrees is an amorphous and evolving issue that "does not neatly fall into the jurisdiction of any single committee."

The report summarizes a series of about a dozen closed-door meetings held by Schumer and his AI group last fall and winter with industry, civil rights and labor leaders, academics and others to get advice and identify areas of consensus for legislating AI safeguards.

"As senators, we acted as moderators, aiming to foster an environment where experts could challenge each other's perspectives in a candid and productive manner," the Schumer group says in the report.

Beyond legislating, the report also encourages committees to work with federal agencies to promote the benefits and manage the risks of AI.

The report "Encourages committees to review forthcoming guidance from relevant agencies that relates to high impact AI use cases and to explore if and when an explainability requirement may be necessary."

Also, the "committees of jurisdiction" are encouraged to "explore ways to ensure that relevant internal and external stakeholder voices, including federal employees, impacted members of the public, and experts, are considered in the development and deployment of AI systems procured or used by federal agencies."

That call for committee action was initially met by the Rules Committee with Chair Amy Klobuchar (D-MN) managing to push through her two bills for protecting elections from deceptive AI content, just hours after the Schumer report was released.

But the committee vote defied the report's call for bipartisanship with both bills, S. 2770 and S. 3875, being approved by 9-2 votes with most Republican members boycotting the markup amid concerns about regulating free speech.

Schumer, who is a member of the committee and voted for the bills, was asked about the partisan vote during a press conference later in the day where he and other members of the AI working group stressed that the report did not endorse any bills on election security.

The report, however, does promote "robust protections in advance of the upcoming election to mitigate AI-generated content that is objectively false, while still protecting First Amendment rights."

At the press conference, Sen. Young said the roadmap calls on committees to consider whether existing laws can be adapted or expanded to address the issues raised by the emergence of AI technologies.

"With this roadmap, we have provided direction to the committees of jurisdiction so they in a bipartisan fashion can consider legislation, some of which we endorse in the roadmap, most of which will be produced in the coming weeks, months and years by our colleagues," Young told reporters.

Schumer noted that the report proposes spending $32 billion over the next several years as a starting point to boost AI research efforts. And Sen. Rounds cited the upcoming annual National Defense Authorization Act as an opportunity for moving AI-related legislation this year.

"Just to follow up on that, just as an example, the NDAA passes every single year, bipartisan in nature, and we try to do our best to keep it as much defense focused as possible," Rounds said.

Other leading legislative vehicles, according to the senators, are the CREATE AI Act, which would authorize and fund a Biden administration pilot research project known as the National AI Research Resource, and the Future AI Innovation Act, which would authorize the U.S. AI Safety Institute at the National Institute of Standards and Technology to develop standards and testbeds for groundbreaking AI to promote U.S. economic and national security.

Both bills are pending before the Commerce Committee.

Beyond the report, senators are being pressed to take action on AI risks to counter foreign adversaries. For instance, Senate Intelligence Chair Mark Warner (D-VA) at a May 15 hearing on election threats said congressional delays were aiding U.S. adversaries.

"And just on a personal note, I fear that Congress's inability to pass any new guardrails in the last eighteen months

for AI-enabled mischief really could pose a huge problem," Warner said in his opening statement.

Similarly, in response to AI roadmap report, Center for Democracy and Technology CEO Alexandra Reeve Givens said it was time to act.

"But after a year of work, Congress needs to do more than acknowledge those issues; it needs to act," Givens said in a statement. "It's not enough to focus on investments in innovation, as the Roadmap does in detail — we also need guardrails to ensure the responsible development of AI."

Government oversight group to oppose inclusion of Peters-Cruz AI procurement bill in NDAA

Posted May 20, 2024

The Project on Government Oversight will oppose a Senate Homeland Security Committee-passed bill intended to ease government AI procurement as lawmakers maneuver to include it in the fiscal 2025 National Defense Authorization Act.

"We're going to push back when it gets thrown in by the [Senate Armed Services Committee] and then at [the NDAA] conference. The idea is to play defense against some of this stuff," Scott Amey, general counsel for the Project on Government Oversight, told *Inside AI Policy* in reference to S. 4066 sponsored by Homeland Security Chairman Gary Peters (D-MI) and Sen. Ted Cruz (R-TX).

The bill sailed out of the Homeland Security Committee without opposition on May 15. POGO is a nonprofit independent watchdog group.

The SASC has scheduled a markup of the fiscal 2025 NDAA for June 12.

The Homeland Security Committee-approved Federal Improvement in Technology, or FIT, Procurement Act would require the director of the Federal Acquisition Institute, housed within the White House's Office of Federal Procurement Policy, to create a training program that would steer contracting officials toward options for buying artificial intelligence and other information and communications technology while bypassing Federal Acquisition Regulations.

The training must inform contracting officials of their ability to use "simplified acquisition procedures" when purchasing artificial intelligence and other information and communication technology, according to text of the legislation.

Such simplified acquisition procedures include "non-FAR based" authorities such as "Other Transaction Authority" contracts approved in 1958 for the National Aeronautics and Space Administration to try out new technologies, and Cooperative Research and Development Agreements which are used to commercialize government-developed technology. The legislation notes these options are available when buying "certain commercial products or services."

Amey said, beyond the tech industry, major federal vendors, particularly those in the aerospace and defense industrial base, often try to increase the range of things that can be purchased under the Simplified Acquisition Threshold, but that is more complicated for services than it is for goods, and software occupies something of a gray area.

"For quite a few years services have outpaced government buying of goods or products," Amey said. "As technologies have taken off, now you have a lot of IT services and I'm sure that this is all gearing up to buy AI services."

"It's a lot easier to buy products. It's much easier to buy a desk or a pen or even a very complex weapon system," Amey said, but "When it comes to services, you're buying labor hours and you're buying, software."

Amey then checked himself. "Actually, I don't know, is software a good, or a service?"

"My guess with this bill, is that they know that there's going to be a lot of buying of innovative services, and that they're trying to have the government be able to do so more quickly, and without the proper shopping mechanisms that ensure the government is getting fair and reasonable prices," he said, adding. "When I read anything that relates to 'commercial products or services,' it looks like it will water down the [acquisition] process and get rid of some of the oversight mechanisms to protect taxpayers."

Responding to the Office of Management and Budget's request for information on what procurement should look like under President Biden's Oct. 30 executive order on artificial intelligence, industry groups said there's nothing special about artificial intelligence that would warrant changing the Federal Acquisition Regulation.

But some of the same companies are backing provisions in the Peters-Cruz bill that say federal rules on payments should be changed to allow for mechanisms such as subscription or rental models under which cloud services are sold.

Among the FAR provisions the exceptions for commercial services would get around are those related to the Truth in Negotiations Act, which requires vendors to provide certified customer pricing data "which companies don't like," Amey said.

Under exceptions for "commercial products or services" under the threshold, he said "[vendors] can just provide any cost or pricing data information or refuse to turn it over."

"In essence [supporters of the bill are] fine with 'let's buy faster, let's make this easier on the contractors thinking that it's going to result in savings," Amey said. "But I never heard [a vendor say] 'oh, you sped this process up so I'm

going to cut my costs.'"

He said "it's a myth because there's no savings on the tail end and what studies have shown is when the government doesn't have the appropriate time to buy, when they don't have the appropriate cost or pricing data in front of them," it leads to "bad deals for taxpayers and a lot of wasted money."

Noting that "something like this hasn't gone through as a standalone in many years," Amey said the group will target "Some of the more taxpayer-friendly members" of the Armed Services committees as the NDAA negotiations get underway.

"The claim is we need to speed up the process, we need to cut red tape and we need competition, that we need non-traditional government vendors to come into the Government Marketplace," he said. "[But] this isn't really all for them. This is for the bigger contractors that want to sell goods and services to the government without having to supply certified cost or pricing data."

CDT issues AI governance guidance on demographic data and bias assessment

Posted May 20, 2024

The Center for Democracy and Technology has released an "AI governance in practice guide" for government and the private sector on the collection of demographic data for use in measuring "fairness and bias" in artificial intelligence systems, stating that historical misuse of such data — to the harm of vulnerable communities — underscores the need for guidelines.

"As governments and policymakers push for fairness in AI, a critical aspect is identifying and mitigating bias. Demographic data plays a pivotal role in this process, but given the risks of misuse, handling that data responsibly is crucial," CDT said in a May 16 release.

"We first look at how to measure demographics, then at how to uncover demographic patterns," CDT said. "To ensure that AI systems serve all communities fairly and responsibly, we urge practitioners to engage with impacted communities, communicate openly, and embed strong technical and institutional safeguards."

The 126-page report, "Navigating Demographic Measurement for Fairness and Equity," was written by CDT's Miranda Bogen.

"As governments and policymakers increasingly expect companies developing and using AI systems to proactively identify and mitigate bias and discrimination, navigating the foundational question of demographic measurement has become critically important," the report said.

"While there is no one-size-fits-all solution, this report makes clear that the lack of obvious access to raw demographic data should not be considered an insurmountable barrier to assessing AI systems for fairness, but neither should it provide a blanket justification for widespread or incautious data collection efforts," it said.

"A variety of creative approaches and safeguards can be used to gain insight into disparate patterns while reducing the risks related to demographic measurement. From exploring privacy-preserving techniques to pursuing measurement of content-related bias when disparities affecting people are hard to measure directly, practitioners have a range of tools at their disposal," according to the report.

It emphasizes that "practitioners must be intentional about the data and methods they adopt in order to prevent the exacerbation of vulnerabilities that marginalized communities already face when it comes to privacy, safety, and dignity. The methods described in this report can be useful to diagnose issues and inform efforts to address biases, but even systems that fare well in measurements could still lead to adverse effects, so mechanisms for accountability and redress will remain relevant and important."

The report calls on regulators to:

• *Recognize that a variety of approaches are available for companies to identify and measure disparities, even in the absence of comprehensive demographic data collection.*

• *Clarify criteria and expectations about acceptable measurement methods when it comes to civil rights compliance, and articulate minimum expectations for how data and methods should be handled.*

• *Explore how more measurement methods can be used to monitor compliance with Federal civil rights laws, including to conduct investigations and enforcement actions.*

• *Facilitate collaboration between NGOs, research institutes, and government data agencies to explore creative ways that existing administrative data can be used to conduct measurements in a privacy-respecting manner.*

• *Encourage continued research to explore how unsupervised, synthetic, privacy-enhancing, and content-related methods can be used to further the detection and remediation of bias and discrimination.*

Practitioners, it said, should:

• *Establish ongoing relationships with communities affected by measurement activities to co-design data collection and handling strategies, discuss potential risks and benefits, and collaboratively define fairness goals.*

• *Where possible, consider methods that avoid generating or storing sensitive demographic information in a way*

that can be easily connected to individuals.

• *Take great care before using observation and inference methods to identify characteristics, especially those lacking precedent or that resist observation.*

• *Clearly differentiate between perceived or implied characteristics and actual ones.*

• *Employ a robust combination of approaches to handling data and measurement methods to ensure appropriate use.*

• *Communicate openly about demographic measurement efforts, as well as how data is handled.*

CDT and other groups recently urged the Office of Management and Budget to make changes to the Federal Acquisition Regulation to require testing systems before and after deployment for harms such as propagating bias against minorities.

CDT on May 15 also released an AI governance-in-practice guide on "applying sociotechnical approaches" to artificial intelligence systems.

"Taking a sociotechnical approach to building and governing AI systems that protect people's rights and safety is increasingly expected by policymakers and public stakeholders and requires thoughtful design of governance, safety, and technical development methods," CDT said in that report.

Comment deadline approaches for generative AI 'profile' under NIST risk management framework

Posted May 20, 2024

Comments are due June 2 on the National Institute of Standards and Technology's draft generative artificial intelligence "profile" crafted under the NIST AI risk management framework and one of the agency's key deliverables called for in President Biden's Oct. 30 executive order on AI.

NIST's AI RMF is one of the federal government's primary tools for addressing AI risks and has been embraced by major industry groups that say it should be foundational to procurement and other policies. The "GAI" profile is an important addition to the RMF aimed at enhancing its usability in government and the private sector.

The initial public draft of NIST AI 600-1, the "GAI" profile, was released in April in a package of draft documents on mitigating AI risks as the Biden administration noted the six-month mark since issuing the executive order on safe and secure AI. The package included NIST's plan for global engagement on standards, a development guide for secure software, and guidance on "reducing risks posed by synthetic content."

All four NIST documents have June 2 comment deadlines.

The generative AI profile is structured around sections on "Risks Unique to or Exacerbated by GAI" and "Actions to Manage GAI Risks." It includes an appendix addressing "primary considerations" such as governance, third-party issues, pre-deployment testing — including limitations of current testing approaches — field testing, red-teaming, content provenance, and incident disclosure.

NIST explains, "Use-case profiles are implementations of the AI RMF functions, categories, and subcategories for a specific setting or application — in this case, Generative AI (GAI) — based on the requirements, risk tolerance, and resources of the Framework user. Consistent with other AI RMF Profiles, this profile offers insights into how risk can be managed across various stages of the AI lifecycle and for GAI as a technology."

The profile identifies a dozen "risks unique to or exacerbated by GAI," ranging from "lowered barriers to entry or eased access to materially nefarious information related to chemical, biological, radiological, or nuclear (CBRN) weapons, or other dangerous biological materials" to confabulation or hallucinations, data privacy, and intellectual property violations.

On information security, it says, "One of the most concerning GAI vulnerabilities involves prompt-injection, or manipulating GAI systems to behave in unintended ways. In direct prompt injections, attackers might openly exploit input prompts to cause unsafe behavior with a variety of downstream consequences to interconnected systems."

The profile explains, "Indirect prompt injection attacks occur when adversaries remotely (i.e., without a direct interface) exploit LLM-integrated applications by injecting prompts into data likely to be retrieved. Security researchers have already demonstrated how indirect prompt injections can steal data and run code remotely on a machine."

It says, "Merely querying a closed production model can elicit previously undisclosed information about that model."

On risk management, it says actions are "organized by AI RMF subcategory," noting that "not all actions apply to all AI actors. For example, not [all] actions relevant to GAI developers may be relevant to GAI deployers. Organizations should prioritize actions based on their unique situations and context for using GAI applications."

Actions are matched to risks in a chart that spans 50 pages.

NIST in an appendix says on pre-deployment testing limitations, "Currently available pre-deployment TEVV processes used for GAI applications may be inadequate, non-systematically applied, or fail to reflect or mismatched to

deployment contexts."

"For example," it says, "the anecdotal testing of GAI system capabilities through video games or standardized tests designed for humans (e.g., intelligence tests, professional licensing exams) does not guarantee GAI system validity or reliability in those domains. Similarly, jailbreaking or prompt-engineering tests may not systematically assess validity or reliability risks."

NIST says, "Measurement gaps can arise from mismatches between laboratory and real-world settings. Current testing approaches often remain focused on laboratory conditions or restricted to benchmark test datasets and in silico techniques that may not extrapolate well to — or directly assess GAI impacts in — real world conditions. For example, current measurement gaps for GAI make it difficult to precisely estimate its potential ecosystem-level or longitudinal risks and related political, social, and economic impacts."

It says, "Gaps between benchmarks and real-world use of GAI systems may likely be exacerbated due to prompt sensitivity and broad heterogeneity of contexts of use."

Activists warn of inherent AI biases in wake of Schumer's legislative 'roadmap'

Posted May 17, 2024

Labor and public interest activists are warning about the inherent racial and other biases in artificial intelligence in response to Senate Majority Leader Charles Schumer's (D-NY) recently released "roadmap" for drafting legislation, arguing the Schumer strategy woefully downplays those risks in favor of business interests.

"And the report today inadequately deals with the elephant in the room, bias in AI. Because foundation models are optimized to reflect their training data . . . we should expect them to reinforce stereotypes," said George Washington University Law Professor Spencer Overton in a scathing review of Schumer's AI roadmap report released May 15.

"And AI in too many situations automates a discrimination . . . effectively acting as a discrimination machine," Overton said, adding that "despite this fact, the 30-page report today used the word innovation 28 times, it used the word bias three times and two of those were in the appendix."

Overton spoke at an event hosted by Public Citizen in a Senate committee room just hours after Schumer and his bipartisan AI working group led by Sens. Mike Rounds (R-SD), Todd Young (R-IN) and Martin Heinrich (D-NM) issued their highly anticipated report intended to guide the chamber's committees in drafting AI legislation.

The Public Citizen "roundtable" discussion included representatives from AI Now, AFL-CIO and National Nurses United and offered a first glimpse at what lawmakers will be facing from labor and public-interest advocates as they navigate trying to draft consensus-based AI legislation.

The assessment of the Schumer report by the panelists stands in stark contrast to the initial glowing reviews offered by the tech industry, which issued multiple statements of strong support for the effort and priorities laid out by the roadmap report.

Participants at the Public Citizen event called for the government to adopt the "precautionary principle" for regulating AI which would ban commercializing an AI technology unless it can be shown to be safe, reliable and free of bias. Also, panelists said Schumer's report falls short in addressing the dominance of big tech in guiding the development of AI technologies that stress profit over societal benefits.

"And I'll note that while the report names very many issues, it's notably silent on competition," said Amba Kak, co-executive director of AI Now.

"And I think there too, we have a pretty well-honed toolkit, everything from prohibiting discrimination by gatekeepers to a rule, for example, that separates the ownership and control of the infrastructure from other related AI markets, is long overdue," she said.

"We're at the point where we can in real time, see the way in which" AI companies and cloud service providers "are essentially consolidating their advantage to control the AI market," she argued.

National Nurses United lead legislative advocate Hannah Bauman said her group is calling on lawmakers and regulators to adopt the precautionary principle long used in the medical and environmental health sciences to require independent scrutiny of AI technologies before allowing them to the market.

"Our union is demanding that the federal government issue AI regulations that are grounded in that precautionary principle," Bauman said. "Tech companies and healthcare employers should be required to prove that AI systems are safe, effective and equitable before these technologies are deployed in healthcare settings. And that is not what is happening right now."

Public Citizen president Robert Weissman echoed that sentiment, saying "we don't have to as a society say, we're going to permit these things, we should say, using the precautionary principle, if we can anticipate they're going to do more harm than good, they should not be permitted to be deployed in the marketplace."

On racial bias in AI, Wasserman said "it's pervasive, whether it's facial recognition, or the deployment of military technologies that are going to replicate racial bias and other forms of bias unless they intentionally are

designed not to do it."

AFL-CIO Tech Institute deputy director Arohi Pathak voiced concern about the pervasive profit-driven approach to designing and developing AI technologies.

"Well, I think technology by itself is not necessarily good or bad. It's how technology is used. It's how it's manipulated," she said.

"I think what we've seen since AI has been running rampant over our society, our communities, our economy over the last however many years that . . . too often corporations will use AI in a way that is exploitive, and they'll do it to maximize their profits," she argued.

"And so why do we live in a society where corporations are allowed to make the rules, and everyone else is okay with that?" Pathak said.

Sen. Cory Booker (D-NJ) kicked off the Public Citizen event by laying out the tremendous benefits and potential risks of AI.

He said the "thought leaders" at the event are "essential to promote AI policies" that "serve the greater public interest and ideals that we share. They're really looking to leverage the upside, be very tech positive, but also make sure that AI doesn't erode workers' rights, erode privacy, enable election interference, or push biases and discrimination."

"I mean, that's really what the call of the moment is," he added.

"And so my hope is that the momentum we seem to have in the Senate, of doing something that we can guide that, and land that in a positive way," he said about pending and emerging legislative proposals for setting guardrails on the development and deployment of AI.

"And to be a part of the architect of how our government responds to this moment is exciting," he added.

The AI policy roadmap issued by Schumer and his bipartisan working group summarizes a series of closed-door meetings last fall and winter with industry, civil rights and labor leaders, among others to identify areas of consensus for promoting the benefits and mitigating the risks of AI with the goal of laying out a path for legislating.

Earlier in the day, the Senate Rules Committee approved on a party-line vote two bills for banning the use of deceptive AI-generated content by political campaigns and labeling AI content, which Public Citizen's Wasserman flagged as an early success of the Schumer roadmap which prioritizes protecting elections.

"It's vital that Congress act on that issue this year," he said.

Consumer advocates calling for AI guidance welcome Supreme Court ruling on CFPB

Posted May 17, 2024

The Consumer Financial Protection Bureau can — and should — now move more confidently to guide the development of artificial intelligence systems following a Supreme Court decision validating its existence, according to advocates trying to incentivize deployers to use less discriminatory alternatives.

"It's really important that anti-discrimination laws are updated to answer the questions that artificial intelligence raises," Adam Rust, director of financial services for the Consumer Federation of America, told *Inside AI Policy* reacting to the May 16 ruling.

The decision comes as CFPB Director Rohit Chopra has taken an active stance on regulating the technology, but also as advocates for consumers, civil rights groups and financial institutions have all called on the bureau to issue more specific guidance regarding the use of "Less Discriminatory Alternatives" to algorithms used to make decisions such as credit approvals.

Rust had posited in January that the lack of guidance from the bureau thus far was due to the outstanding decision from the high court which has now opined on the constitutionality of CFPB's funding mechanism.

"I think it's important that they provide at least examples of ways to do things well, because I think there will be lenders out there that claim they're doing something well, even if there's really no basis at all for that," Rust said. "We don't want fairness through unawareness."

Rust said if the case had been decided differently, it would have "essentially put the CFPB in suspended animation" and disrupted "any new work it would have done on something like AI, for rulemaking, or even potentially things like guidance."

The White House, which has twice through executive order on artificial intelligence encouraged the CFPB to uphold civil rights laws like the Equal Credit Opportunity Act amid the threat of algorithmic discrimination, also celebrated the decision.

"Today's Supreme Court ruling is an unmistakable win for American consumers," reads a May 16 statement from the White House. "The CFPB has worked to protect consumers from abusive practices by lenders, servicers, and special interests."

"Republicans in Congress and in states across the country have stood with special interests who want to keep ripping families off," the statement continued. "In the face of years of attacks from extreme Republicans and special

interests, the Court made clear that the CFPB's funding authority is constitutional and that its strong record of consumer protection will not be undone."

Rust said a different decision from the court "might have meant [the question of the bureau's authorities] would have to go back to Congress" where the political climate is stormy.

"Despite the setback from today's ruling, Republicans will continue the fight to rein in the rogue CFPB," said House Financial Services Chairman Patrick McHenry (R-NC) in a May 16 release. "To be clear, this Supreme Court opinion yet again emphasizes that Congress has exclusive authority and discretion over federal agencies' funding structures."

"The House must urgently take up Congressman Andy Barr's (R-KY) CFPB Transparency and Accountability Reform Act," McHenry said. "This commonsense legislation will fix the mistakes of Dodd-Frank which set the dangerous precedent of tapping the central bank to fund partisan political objectives. It's past time the CFPB is held accountable to the American people through their elected representatives."

House Foreign Affairs reschedules markup of AI export-controls bill to add White House input

Posted May 17, 2024

The House Foreign Affairs Committee has postponed consideration of a bill that would authorize the president to control the release of artificial intelligence models with the aim of limiting their access by foreign adversaries, so it can be revised to reflect feedback from the White House.

"Our negotiations with the [administration] bore some last-minute fruit and now we need to incorporate that," the committee's press office told *Inside AI Policy*. H.R. 8315 will now be marked up May 22, according to the committee.

Introduced by Foreign Affairs Chairman Michael McCaul (R-TX), the bill has a string of bipartisan cosponsors who have been successful in advancing bills such as the ostensible ban on TikTok while warning of Beijing's military ambitions associated with the technology.

The Enhancing National Frameworks for Overseas Restriction of Critical Exports, or ENFORCE Act — initially scheduled for markup May 16 — could have particularly significant implications for open source AI models and innovation, according to tech industry and public interest groups.

The Linux Foundation, a nonprofit open-source advocacy organization, has noted, "under the [Export Administration Regulation], the term 'export' has a broad meaning."

"The simple act of releasing technology to someone other than a US citizen or lawful permanent resident within the United States is deemed to be an export, as is making available software for electronic transmission that can be received by individuals outside the US," reads guidance the foundation shared in releasing a 2020 report on how to navigate export controls on certain forms of encryption. Export controls cannot apply to anything that has been openly "published" the foundation noted at the time.

The McCaul bill gives the president the power to require a license from the Commerce Department's Bureau of Industry and Security to engage in "activities that may support the design, development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing of" covered artificial intelligence systems.

Legal dispute over OpenAI documents may come to a head in landmark copyright suit

Posted May 17, 2024

Class-action plaintiffs are asking a federal district court for a meeting with defendants OpenAI and Microsoft to resolve a dispute over access to documents about the training of generative artificial intelligence models, which plaintiffs say will show that the companies' knowingly violated copyright protections.

"To date, OpenAI has produced only 46 documents and Microsoft has produced 0 documents. Of the 46 documents produced, nearly all of them (78%) are documents that can be downloaded from the internet, like blogposts from OpenAI's website," says a May 15 letter from plaintiffs' attorneys to the U.S. district court for southern New York to request a "conference."

The request is the latest development in a simmering dispute by parties in *Authors Guild et al. v. OpenAI et al.* over access to documents during the discovery phase of the lawsuit.

The dispute underscores how important information about how AI developers train their generative models has become among the various copyright infringement cases recently filed against the industry.

Plaintiffs in Authors Guild are raising concerns with the court that defendants appear to be trying to run out the clock in an effort to deny or limit access to the requested information.

"With just four months remaining before the discovery cutoff, and less than a month before the June 14, 2024 substantial completion deadline, the Court's intervention is necessary to hold all parties accountable to the current

schedule," the latest filing states.

"To that end, Plaintiffs propose the following: A case management conference before Your Honor to address the status of discovery and measures proposed herein; Bi-weekly discovery conferences to address the status of discovery and any discovery disputes among the parties; [and] Bi-weekly status reports filed with the Court, in advance of any discovery conferences, identifying all issues that are the subject of the parties' meet and confer efforts and the status of those efforts," the letter says.

Plaintiffs on May 14 filed a proposed "stipulated protective order" to allow the companies to protect proprietary information.

"For Protected Discovery Material designated 'HIGHLY CONFIDENTIAL — SOURCE CODE,' the following additional restrictions apply: (a) Access to a Party's Source Code Material shall be provided only on 'standalone' computer(s) (that is, the computer may not be linked to any network, including a local area network ('LAN'), an intranet or the Internet) . . . .(b) The receiving Party shall make reasonable efforts to restrict its requests for such access to the stand-alone computer(s) to normal business hours, which for purposes of this paragraph shall be 8:30 a.m. through 6:00 p.m, Monday through Friday, local time where the stand-alone computer(s) are physically located, excluding any local holidays . . . .[and] (c) The receiving Party shall provide the producing Party with notice of its intent to inspect the stand-alone computer(s) at least five business days prior to any inspection. The notice may state that the review will continue from day-to-day as needed," says the proposed order in addition to 13 other provisions for protecting "source code material."

Plaintiffs earlier this month accused OpenAI of deliberately withholding information about the data it used to train its generative AI models.

"OpenAI's compilation and use of these two important books datasets — potentially including books from notorious pirated book websites — to train its Large Language Models ('LLMS's') and decision subsequently to delete all copies of these datasets are facts to which the public should have access," argued plaintiffs in a May 6 filing with the New York federal court.

"OpenAI's request to redact information about these datasets, books1 and books2, should be denied for multiple reasons," plaintiffs told the court.

NIST draft plan for global engagement on AI standards sets stage for international collaboration

Posted May 17, 2024

The National Institute of Standards and Technology's draft plan for international collaboration on standards for artificial intelligence technologies, crafted under an AI executive order and currently open for comment, identifies challenges in standards development for the AI space and is intended to help guide engagement with partners, competitors and standards-making bodies.

NIST issued the draft "Plan for Global Engagement on AI Standards" in April and is accepting comments through June 2. The plan was released with three other draft documents on mitigating risks around artificial intelligence systems on April 29 as the Biden administration highlighted the six-month mark since issuing its wide-ranging Oct. 30 executive order on safe and secure AI.

"The [global engagement] plan calls for a coordinated effort to work with key international allies and partners and with standards developing organizations to drive the development and implementation of AI-related consensus standards, cooperation and coordination, and information sharing," according to the draft strategy.

The 29-page draft discusses the objectives for engagement on AI standards, lists priority topics, and offers recommended activities. It includes an appendix on "standards in relation to AI" that discusses how AI standards differ from other technical standards, and another appendix on the current standards landscape.

According to NIST, "This plan furthers the policies and principles in [EO 14110] which instructs the Federal government to 'promote responsible AI safety and security principles and actions with other nations, including our competitors, while leading key global conversations and collaborations to ensure that AI benefits the whole world, rather than exacerbating inequities, threatening human rights, and causing other harms.'"

NIST says, "By advancing global AI standards with these goals in mind, the U.S. government seeks to assist both the private and public sectors to seize the benefits of AI while managing risks to people domestically and across the globe."

The plan is "guided by principles set out" in NIST's AI Risk Management Framework and the federal government's National Standards Strategy for Critical and Emerging Technology, NIST says.

NIST notes that, "while some AI standards will be required by government regulations, their effectiveness generally will depend on organizations to voluntarily adopt those standards — which they will do only if they find the relevant standards implementable and useful."

"New standards typically are based on novel discoveries and technical insights from scientific research and innova-

tion," according to the document. "The more grounded a standard is in the underpinning science, the more implementable and useful it will be for the global AI community, and the greater its chances of international adoption."

"Conversely," the document says, "a standard that attempts to get ahead of the underpinning science may be built on less rigorous technical foundations, may prove unhelpful, or even counterproductive or technically incoherent. The same holds true for related tools."

NIST says, "AI standards will be most useful if they respond to the needs of a diversity of potential users around the world. Standards are most likely to achieve this if they are:"

Context-sensitive, providing flexibility to enable adoption by small, medium, and large entities in their own contexts of use; Performance-based, providing flexibility by focusing on outcomes rather than prescribing specific ways of achieving those outcomes; Human-centered, accounting for human needs, interactions, and values; and Sensitive to societal considerations that may arise from the design, development, deployment, or use of the technologies.

The agency also notes that "the U.S. Government remains committed to protecting human rights in all its activities, including standards-setting for emerging technologies such as AI."

Biden administration issues workplace principles for AI under directive in executive order

Posted May 16, 2024

The Biden administration has issued a set of eight principles for the development and deployment of artificial intelligence in the workplace under the Oct. 30 executive order on AI, highlighting commitments from Microsoft and the jobs site Indeed, while signaling that the Labor Department will follow up with guidance on "best practices."

President Biden's sweeping executive order included "direction for the Department of Labor to establish a set of key principles that protect workers and ensure they have a seat at the table in determining how these technologies are developed and used," according to a May 16 White House announcement.

"The Biden-Harris Administration is today unveiling these principles and announcing that technology companies Microsoft and Indeed have committed to adopt these principles as appropriate to their workplace," the White House said.

"Workers must be at the heart of our nation's approach to AI technology development and use," said Acting Labor Secretary Julie Su. "These principles announced today reflect the Biden-Harris administration's belief that, in addition to complying with existing laws, artificial intelligence should also enhance the quality of work and life for all workers. As employers and developers implement these principles, we are determined to create a future where technology serves the needs of people above all."

The Labor Department said in a release, "Specifically, the AI principles emphasize ethical development; transparency in its use; meaningful worker engagement in system design, use, governance and oversight; protection of workers' rights; and use of AI to enhance work."

Labor said, "The department remains committed to monitoring AI's impact on the workforce and partnering with companies, unions, and other stakeholders to protect and empower workers. As part of this effort, the department will soon provide employers and developers with best practices to consider as they implement the AI principles."

The principles are:

- *Centering Worker Empowerment: Workers and their representatives, especially those from underserved communities, should be informed of and have genuine input in the design, development, testing, training, use, and oversight of AI systems for use in the workplace.*
- *Ethically Developing AI: AI systems should be designed, developed, and trained in a way that protects workers.*
- *Establishing AI Governance and Human Oversight: Organizations should have clear governance systems, procedures, human oversight, and evaluation processes for AI systems for use in the workplace.*
- *Ensuring Transparency in AI Use: Employers should be transparent with workers and job seekers about the AI systems that are being used in the workplace.*
- *Protecting Labor and Employment Rights: AI systems should not violate or undermine workers' right to organize, health and safety rights, wage and hour rights, and anti-discrimination and anti-retaliation protections.*
- *Using AI to Enable Workers: AI systems should assist, complement, and enable workers, and improve job quality.*
- *Supporting Workers Impacted by AI: Employers should support or upskill workers during job transitions related to AI.*
- *Ensuring Responsible Use of Worker Data: Workers' data collected, used, or created by AI systems should be limited in scope and location, used only to support legitimate business aims, and protected and handled responsibly.*

"These principles should be considered during the whole lifecycle of AI — from design to development, testing, training, deployment and use, oversight, and auditing. The principles are applicable to all sectors and intended to be mutually reinforcing, though not all principles will apply to the same extent in every industry or workplace," the White House says.

"The principles are not intended to be an exhaustive list but instead a guiding framework for businesses. AI devel-

opers and employers should review and customize the best practices based on their own context and with input from workers. The Administration welcomes additional commitments from other technology companies who wish to adopt these principles," according to the White House.

Microsoft vice chair and president Brad Smith posted on LinkedIn, saying, "These principles provide a roadmap to help usher in a new era of technological transformation, one that will serve the country's workers. AI holds the promise to change the way we live and work, when implemented responsibly. Microsoft is committed to supporting workers and advancing the principles outlined today."

Chris Hyams, CEO of Indeed, said in a statement, "The Administration's new principles for AI in the workplace are an important step forward in supporting the responsible creation and use of AI for the benefit of US workers. These principles offer an important guide as all parties collectively move forward to protect workers while also enabling innovation."

Hyams said, "The benefits of AI to help workers find jobs and to do their jobs better are tremendous, however proper AI system safeguards must be in place to appropriately protect workers' rights. Indeed greatly appreciates the Administration and Department of Labor's AI leadership and looks forward to further efforts to help people get jobs responsibly and effectively."

Microsoft and LinkedIn this week also released their "2024 Work Trend Index Annual Report" focusing on AI in the workplace.

"While leaders agree AI is a business imperative, many believe their organization lacks a plan and vision to go from individual impact to applying AI to drive the bottom line. The pressure to show immediate ROI is making leaders inert, even in the face of AI inevitability," according to the report.

"To help leaders and organizations overcome AI inertia, Microsoft and LinkedIn looked at how AI will reshape work and the labor market broadly, surveying 31,000 people across 31 countries, identifying labor and hiring trends from LinkedIn, and analyzing trillions of Microsoft 365 productivity signals as well as research with Fortune 500 customers," the report says.

Sen. Warner says delay on AI legislation aids election disruptions by foreign adversaries

Posted May 16, 2024

Senate Intelligence Chair Mark Warner (D-VA) warned that congressional delays in enacting legislation to protect elections has enabled foreign adversaries to leverage emerging artificial intelligence technologies against the U.S. and its allies.

"And just on a personal note, I fear that Congress's inability to pass any new guardrails in the last eighteen months for AI-enabled mischief really could pose a huge problem," Warner said in his opening statement at a May 15 Intelligence Committee hearing on foreign threats to this year's elections.

Warner said the hearing was the first in a series to inform the public and policymakers about emerging and persistent foreign threats to global elections and democratic institutions.

His hearing was held on the same day that the Senate Rules Committee approved election security legislation including a ban on the use of deceptive AI-generated content by campaigns, and the release of Majority Leader Charles Schumer's (D-NY) AI policy "roadmap" which ranks protecting elections among its top priorities.

At the Rules Committee markup, Warner cited the Munch Security Conference in February where dozens of big tech companies pledged action to make sure their platforms and services are not being used to disrupt elections.

"Well, that is all well and good. And there was much fanfare in Munich about this announcement," Warner said to argue that, to date, those tech companies have failed to demonstrate they are living up to those pledges.

"Where are the actions that they are taking to take down content" intended to manipulate activity, he said.

"Unfortunately, I don't think voluntary guardrails are enough, as we've seen from the Munich accord, again much bandied about by the tech companies, but we've not seen specific actions taken," he said in explaining his support and vote for the legislation approved by the Rules Committee.

At Warner's hearing, National Intelligence Director Avril Haines said emerging AI technologies are fueling a growing threat to U.S. and other elections taking place this year around the world.

"Using every tool we have is critical, as the challenge is expanding. Over the last several years, we've seen three trends that make the threat landscape more diverse and complex," Haines told the committee.

"First, our adversaries are more incentivized than ever to intervene in our elections because they can understand that it could affect their particular national interest," she said.

"Second, there are more commercial firms through which state actors are able to conduct election influence activities, often increasing the sophistication of such activities while making it more challenging to track down the original instigator of foreign influence efforts," she added.

And third, "perhaps most obviously, relevant emerging technologies, particularly generative AI and big data analytics, are

increasing the threat by enabling the proliferation of influence actors who can conduct targeted campaigns, reducing the cost of relatively sophisticated influence operations and content, and further complicating attribution," she warned.

Singling out China, Haines said Beijing has "a sophisticated influence apparatus through which they leverage emerging technologies, including generative AI, and they are growing increasingly confident in their ability to influence elections globally but remain concerned about possible blowback in the event their efforts are disclosed."

FBI Executive Assistant Director Larissa Knapp told the committee that generative AI has made it easier for adversaries to wreak havoc on the election process.

"Advancement in cyber capabilities and technology presents new challenges for the FBI in combating the threats to election security," Knapp said.

Generative AI has "lowered the threshold for foreign adversaries to create fake accounts and media that can be used to amplify false narratives," she said.

"This increases the capability of our less sophisticated adversaries and provides our already sophisticated adversaries a powerful tool to increase the scale and efficiency of their election influence operations," Knapp warned.

Cybersecurity and Infrastructure Security Agency Director Jen Easterly also testified, telling senators that her agency released guidance in January "which provides an overview of how generative AI-enabled capabilities are often used by malicious actors to target the security and integrity of election infrastructure, and basic mitigations to address these threats."

A day before the hearing, Chair Warner sent letters to major tech companies asking them to report to the committee by May 24 on actions they are taking to ensure their AI technologies are not being used to undermine democratic institutions and elections.

"Against the backdrop of worldwide proliferation of malign influence activity globally — with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions," Warner wrote in May 14 letters to tech firms, asking them to detail "specific measures" they are taking to implement the commitments they made at the Munich conference.

"While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy — and durability — of the initiatives and protection measures you adopt," Warner wrote in his letters in an apparent attempt to assess where additional legislation might be needed.

Industry-backed bill to boost federal AI procurement clears Senate Homeland panel

Posted May 16, 2024

The Senate Homeland Security Committee favorably reported S. 4066, a bill that would make it easier for federal contracting officers to buy artificial intelligence products and other goods and services considered commercial information and communications technology.

The panel voted May 15 on the Federal Improvement in Technology (FIT) Procurement Act which was introduced by Homeland Security Chairman Gary Peters (D-MI) and Sen. Ted Cruz (R-TX).

Peters and Cruz recently said the bill would "strengthen training for the federal acquisition workforce to ensure they are best prepared to manage the purchase of rapidly advancing technologies, such as artificial intelligence systems."

The legislation is advancing as implementation of President Biden's Oct. 30 executive order on artificial intelligence hinges substantially on the government's procurement posture. The Office of Management and Budget is now reviewing public comments on how it should guide federal agencies' acquisition practices to safeguard individuals' rights and safety under the order.

Civil society groups have urged OMB to amend federal regulations so they reflect the unique attributes of artificial intelligence systems and require appropriate testing. They also argue that amid heavy marketing by AI vendors, which is unlikely to highlight accompanying risks, agencies should conduct a needs assessment before issuing any solicitation.

In contrast, major industry groups pointed to provisions in the Federal Acquisition Regulation that suggest defaulting to commercial off-the-shelf items and told OMB "quality assurance" testing conducted by vendors themselves under current regulations is sufficient to manage AI risks.

In this vein, the bill from Peters and Cruz — who highlighted supportive statements they received from the Information Technology Industry Council and the Professional Services Council — echoes the industry perspective.

It instructs the director of the Federal Acquisition Institute, which is housed by OMB's Office of Federal Procurement Policy, to design a training program for certifying contracting officials that "include[s] learning objectives that encourage the use of commercial or commercially available off-the-shelf technologies to the greatest extent practicable."

Among other things, the bill would also give the administrator of the OFPP the power to eliminate parts of the Federal Acquisition Regulation based on a working group required to "obtain input from the public, including from the APEX Accelerators program (formerly known as Procurement Technical Assistance Center network) and other contrac-

tor representatives," according to text of the legislation.

The goal of the working group would be to "identify Federal procurement policies and regulations that are obsolete, overly burdensome or restrictive, not adequately harmonized, or otherwise serve to create barriers to participation in Federal contracting or unnecessarily increase bid and proposal costs." The administrator, who chairs the Federal Acquisition Regulatory Council, must then implement the regulatory and non-legislative actions identified within two years of the bill's enactment.

The bill would also double the Simplified Acquisition Threshold — "the threshold under which agencies may use simplified acquisition procedures to reduce costs, improve opportunities for qualified businesses, promote efficiency and economy, and avoid unnecessary burdens for agencies and their contractors" — from $250,000 to $500,000 and allow agencies to pay providers of cloud services and other information and communications technology in advance, on a "subscription, reservation or tenancy basis."

The bill passed out of committee unopposed.

Klobuchar's election security bills are first wins under Schumer's AI 'roadmap'

Posted May 16, 2024

The Senate Rules Committee approved along party lines two of Chair Amy Klobuchar's (D-MN) legislative proposals for protecting elections from the threat of artificial intelligence, after Majority Leader Charles Schumer's (D-NY) bipartisan "roadmap" for legislating AI safeguards was released on the same day with a call for protecting elections.

"And so as we head into this election, I would argue 'the hair on fire' moment is that we actually take this on immediately and not wait," said Klobuchar about the need to pass the bills.

The committee on May 15 approved by 9-2 votes S. 2770, the Protect Elections from Deceptive AI Act, and S. 3875, the AI Transparency in Elections Act, with all Democrats on the committee voting for the bills and most Republicans skipping the markup. Ranking member Deb Fischer (R-NE) and Sen. Roger Wicker (R-MS) voted against both bills.

Schumer, who is a member of the committee, voted for both bills saying his roadmap report "supports these proposals." Senate Minority Leader Mitch McConnell (R-KY) is also member of the committee, but he skipped the markup along with most other Republicans.

Klobuchar said there is bipartisan support for the bills "outside the committee" and that she expects the Senate to take up the measures in the "next few months."

The committee also unanimously approved S. 3897, the Preparing Election Administrators for AI Act, which requires the U.S. Election Assistance Commission to develop guidelines for local and state election officials on mitigating AI risks and to study the effects of AI on the upcoming election.

Klobuchar touted S. 2770 for banning deceptive AI-generated content by campaigns and their allies and S. 3875 for labeling AI-produced political ads as simply codifying on the federal level what a number of state legislatures controlled by either Democrats or Republicans have already adopted.

In response to the growing threat from AI-generated content, Klobuchar said "many states have come to the rescue, but they can only do their own state ads, and their own state robocalls, and their own state videos," leaving federal elections unprotected.

"At least 14 states have now enacted some form of labeling [requirement] so that at least the viewers of these videos know if they're real or not, if it's the real person or not," she said. "And several have looked at or adopted bans, including the state of Texas, which unanimously in their legislature, passed a ban with the support of Governor Abbott," a prominent conservative, she added.

But ranking member Fischer rejected that call to action, arguing that the bills would inappropriately federalize the administration of national elections, violate the constitutional protections for free speech and go beyond many of the state restrictions being touted by Democrats in support of the bills.

"As we discussed in a hearing last year, the issues surrounding AI and elections are complicated. We have to balance the potential for innovation, with the potential for deceptive or fraudulent use. On top of that, we can't lose sight of the important protections our Constitution provides for free speech in this country. These two bills do not strike that careful balance," Fischer said before the votes.

Despite the committee's passage of the bills, the tensions over free-speech restrictions and the role of the federal government in protecting state-run elections foreshadow future challenges for proponents of the legislation as they potentially move to Senate floor votes.

Both Schumer and Klobuchar described the committee's votes as "excellent" by clearing the bills for further consideration in the Senate and potentially setting up the first floor debate on AI legislation backed by Schumer's bipartisan roadmap.

"The AI Working Group encourages the relevant committees and AI developers and deployers to advance effective watermarking and digital content provenance as it relates to AI-generated or AI-augmented election content," says the

report by Schumer's bipartisan group.

"The AI Working Group encourages AI deployers and content providers to implement robust protections in advance of the upcoming election to mitigate AI-generated content that is objectively false, while still protecting First Amendment rights," says the report in potentially framing the upcoming Senate debate on S. 2770 and S. 3875.

FTC's Khan emphasizes AI efforts in appearance before House appropriators

Posted May 16, 2024

Federal Trade Commission Chair Lina Khan stressed artificial intelligence initiatives, as well as broader work on data security and privacy, as she made her case for increased funding in May 15 testimony before House appropriators.

"The rapid emergence of new tools powered by artificial intelligence ("AI") presents opportunities for consumers, workers, and our economy. But it also poses significant risks, and the Commission is working to address these risks in a number of ways while also promoting innovation that affirms America's leadership around this emerging technology," Khan testified before the House Appropriations financial services and general government subcommittee.

Subcommittee Chair David Joyce (R-OH) began the session with a warning that the FTC was unlikely to receive the budget increase it is seeking. "The Fiscal Year 2025 budget request for the Federal Trade Commission is $535 million dollars. That would require a nearly 35 percent plus up from the Fiscal Year 2024 enacted level," he said.

"Now, I'll be honest," Joyce said, "it would be difficult to support a 35 percent increase at the FTC or any agency under our jurisdiction. Current government spending levels are unsustainable. We have seen record deficits in recent years, in part due to COVID, and we have to reduce our spending. Under this Administration, the FTC has prioritized the issuance of many polarizing regulations that push the legal boundaries of the Commission's mission as established by Congress."

Subcommittee ranking member Steny Hoyer (D-MD) argued in favor of the funding boost, saying, "FTC rules help defend Americans against everything from scam calls to health care data breaches."

The FTC in a press release said, "For FY 2025, the Commission has requested $535 million. This increase would help fund mandatory FY 2024 and anticipated FY 2025 pay increases and other inflationary non-pay expenses, as well as critical IT investments needed for the Commission to continue its enforcement work in an era of big data."

Khan in her testimony said the "full scope" of the commission's work "reflects Congress's decision to charge the FTC with enforcing or administering the provisions of more than 80 statutes."

"I am deeply committed to ensuring that the FTC's efforts to carry out the tasks Congress assigned us makes best use of the resources Congress has granted us, which is why the agency prioritizes addressing dominant actors and upstream facilitators of widespread harm, rather than playing whack-a-mole; seeks to deter unlawful activity from the start; and strives to be forward-looking in anticipating problems, especially as it relates to emerging technologies and nascent markets across sectors," Khan said.

Khan ran through an extensive list of consumer data security efforts underway at the commission as well as actions taken "when biometric technologies, like facial recognition, harm consumers." She also detailed data privacy and children online protection initiatives.

In a section of her testimony titled "Confronting the Challenges of Artificial Intelligence," Khan said "the Commission is using its existing legal authorities to take action against illegal practices involving AI."

"For instance," she said, "the FTC alleged that Amazon and Ring used highly private data — voice recordings collected by Amazon's Alexa voice assistant and videos collected by Ring's internet-connected home security cameras — to train their algorithms while violating customers' privacy."

Further, Khan said, "the Commission is using every tool to fight AI-related fraud. The Commission has issued a rule outlawing government and business impersonation scams — a type of fraud that generative AI can turbocharge. The Commission has also embarked on a supplemental rulemaking to extend this ban to the impersonation of individuals."

And, she said, "the Commission is helping guide consumers and businesses as they navigate the potential perils of AI. The Commission has issued award-winning consumer and business guidance around various AI-related issues."

"Finally," Khan said in this section of her testimony, "the Commission wants to ensure that biometric information — a particularly sensitive category of health data — is being protected, and in 2023, issued a policy statement identifying factors the FTC will consider in determining whether business' use of biometric information or biometric information technologies, including those powered by AI and machine learning, could be unfair in violation of the FTC Act."

Khan also pointed out that in November 2023, "the FTC staff published a summary of responses from the RFI on cloud computing. The Commission is gathering information to inform our understanding of key features of cloud computing; the potential for outages from large cloud providers to have widespread impact on large parts of the economy; security risks; and issues related to market power and business practices affecting competition."

"In January," she said, "the Commission launched an inquiry into generative AI investments and partnerships, issuing orders to five companies requiring them to provide information regarding recent investments and partnerships involving generative AI companies and major cloud service providers. The agency's 6(b) inquiry will scrutinize corporate partnerships and investments with AI providers to build a better internal understanding of these relationships and

their impact on the competitive landscape."

Khan highlighted the work of the FTC Office of Technology established in 2023, saying, "OT's contributions in its first year have been significant."

"In addition to issuing a Cloud Computing RFI that identified both competition and consumer protection issues for further study, OT contributed to the launch of an inquiry into generative AI investments and partnerships amid a quickly evolving marketplace to better understand these relationships and their impact on competition," Khan said.

"In January 2024, the team hosted the first ever FTC Tech Summit on Artificial Intelligence, which encompassed a series of conversations across the layers of the AI technology stack — from chips and cloud infrastructure to data and models to consumer facing applications," she testified.

The FTC on May 15 released its 2023 annual report with a focus on AI-related efforts.

"As artificial intelligence and algorithmic decision-making tools proliferated, the FTC's enforcement and policy efforts have been forward-looking — enabling the agency to stay on the cutting edge as these technologies develop," the commission said in a statement.

Readout from U.S.-China AI meeting cites 'candid and constructive' discussion on risk management

Posted May 16, 2024

U.S. and Chinese officials on May 14 met in Geneva on artificial intelligence "risk and safety," with an exchange of views on approaches and priorities under a dialogue agreed to at the November 2023 summit between President Biden and President Xi Jinping.

"The United States affirmed the need to maintain open lines of communication on AI risk and safety as an important part of responsibly managing competition," according to a readout provided by the National Security Council.

"In a candid and constructive discussion, the United States and [the People's Republic of China] exchanged perspectives on their respective approaches to AI safety and risk management," according to an NSC spokesperson. "The United States reiterated the importance of harnessing the benefits of AI for sustainable development, for developing and developed& countries alike."

Further, the spokesperson said, "The United States underscored the importance of ensuring AI systems are safe, secure, and trustworthy in order to realize these benefits of AI, and of continuing to build global consensus on that basis. The United States also raised concerns over the misuse of AI, including by the PRC."

The U.S. side was represented by Special Assistant to the President and Senior Director for Technology and National Security Tarun Chhabra and State Department Acting Special Envoy for Critical and Emerging Technology Seth Center, along with other officials from the White House, the Department of State, and the Department of Commerce.

The PRC delegation included officials from the Ministry of Foreign Affairs, Ministry of Science and Technology, National Development and Reform Commission, Cyberspace Administration of China, Ministry of Industry and Information Technology, and the Chinese Communist Party Office of the Central Foreign Affairs Commission, according to the NSC readout.

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

"We're not looking to develop a joint statement. This is an exchange of views, and . . . our national security measures are not up for negotiation," an administration official said in advance of the Geneva meeting.

Industry finds benefits, activists focus on potholes in Sen. Schumer's AI 'roadmap'

Posted May 15, 2024

Industry groups see extensive benefits in Senate Majority Leader Charles Schumer's (D-NY) "roadmap" for advancing artificial intelligence policy, especially in areas of research and perhaps in heading off a European Union-style AI regulatory regime, while a digital rights group denounced the report's approach as largely a giveaway to the tech sector.

Schumer's bipartisan AI working group on May 15 released a report summarizing last year's closed-door Senate "insight forums" with industry, civil rights and labor leaders, academics, and other stakeholders, and laying out a roadmap for legislation on safe uses and promoting the benefits of AI. The working group includes Schumer and Sens. Mike Rounds (R-SD), Martin Heinrich (D-NM) and Todd Young (R-IN).

Schumer stressed the diversity of input that his bipartisan AI working group received, telling reporters on May 15,

"We had experts from all walks of life, people, of course from the tech industry, but people from the civil rights community and the labor community and critics of AI, all coming together and actually talking to each other. And coming up with both questions we had to answer and solutions to some of those questions."

Schumer said, "We've been clear from the beginning that this process was meant to supplement not supplant the committee process. We always knew we would have to go to the committees to get the specifics done. And there's so many different aspects of AI in so many different areas that it would take many committees to do it."

BSA welcomes roadmap

Among the industry statements, BSA-The Software Alliance CEO Victoria Espinel said, "BSA commends Leader Schumer, and Sens. Rounds, Heinrich, and Young for their serious and bipartisan work to advance artificial intelligence (AI) policy in the United States."

She said, "The Senate's bipartisan roadmap for AI policy places a welcome focus on promoting innovation in technology and recognizes the benefits of AI across the economy and society. BSA welcomes the roadmap's support for a risk-based approach to AI, and its call for action on a strong and comprehensive privacy law to protect the personal data of consumers nationwide."

Espinel said the roadmap "supports the ability of small businesses to better leverage cloud infrastructure and AI, recognizes the important role of federal procurement in setting rules for AI, promotes the use of content authentication tools, and underscores the need for enabling the trusted free flow of information across borders."

And, she said, "The roadmap additionally calls for action that would help to advance standards work, including through investments in [the National Institute of Standards and Technology], and the development of tools to test AI systems."

Publication of the roadmap "should now provide an impetus for action on legislation. National technology laws remain the best way to widely spread the benefits of responsible AI and build trust and adoption, especially as U.S. states begin to act on AI legislation," Espinel said.

Center for Data Innovation

Hodan Omaar of the industry-based Center for Data Innovation said, "This roadmap for AI policy shows Congress is listening to those who have called on policymakers to ensure the United States remains the global leader in AI. By investing in and prioritizing AI innovation, the United States is helping safeguard its position and creating a framework for policy that recognizes the enormous societal and economic benefits AI can bring to sectors such as health care, transportation, and education."

The center is part of the nonprofit Information Technology and Innovation Foundation.

"The roadmap will help the United States steer clear of the pitfalls Europe is encountering. EU policymakers have failed to prioritize AI innovation and adoption and plunged into a stringent regulatory regime that now has them worrying if they have shot themselves in the foot and will ever be able to catch up with the U.S. economy," Omaar said. "The roadmap suggests Congress is learning from that cautionary tale."

"However," Omaar said, "this roadmap is designed to spur a wave of legislative activity in Congress to address concerns about AI — privacy, safety, workforce disruptions, etc. — and the challenge for Congressional lawmakers will be to pick the right policy solution for each concern. They should recognize that certain issues may require new regulations, but many can be addressed by legislation that sets guidelines, promotes certain practices, or incentivizes desired behaviors."

Omaar cited a House-passed bill "supporting the development of privacy-enhancing technologies" as a "great example of non-regulatory legislation that will help address some of the privacy concerns related to AI."

Omaar said, "Finally, the roadmap leans heavily on investments to support AI research and development, but policymakers should recognize that the benefits of AI are not going to be realized by only improving AI development. The United States also needs a multipronged national AI adoption plan to ensure these opportunities are translated into all the areas where they can make a positive difference in people's lives. It is therefore critical that Congress focus on crafting policies that accelerate the adoption of AI in both the public and private sectors."

TechNet

TechNet president and CEO Linda Moore said, "AI has the potential to help us solve the greatest challenges of our time, from health care, agriculture, and education to transportation, energy, and national security, which we highlight in our AI for America initiative. However, recognizing and addressing the genuine risks associated with AI is crucial for its responsible advancement. By addressing these concerns head-on, we can ensure we're maximizing its benefits for all Americans."

She said, "The U.S. must be the global leader in AI investment, development, and deployment to ensure it is implemented safely across the world. The Senate's AI Roadmap will strengthen America's global competitiveness in AI and emerging technologies. By providing robust funding for the U.S. AI Safety Institute, the National AI Research Resource (NAIRR), the Regional Innovation and Technology Hubs program, retrofitting NIST laboratories for the modern era, and other key priorities, Congress will empower a new generation of AI leaders, expand innovation and

opportunity beyond Silicon Valley, and keep America at the forefront of scientific development for generations to come."

According to Moore, "The Senate AI Roadmap will bolster our workforce through investments in upskilling and training programs and our ability to attract and retain the world's best talent, policies TechNet has long championed and that are needed to counter actions being taken by our foreign competitors. It also urges the passage of the CREATE AI ACT, which would authorize the NAIRR and lower the barrier to entry for AI research. TechNet has worked with Rep. Anna Eshoo (D-CA) to advocate for the bill's passage."

Moore said, "The roadmap acknowledges the importance of implementing AI guardrails to protect our democratic institutions, including preventing political candidates and their agents from using AI to release misleading campaign content. It also recommends policies that further the tech industry's long-standing partnership with the military to advance U.S. national security objectives."

Activists reject roadmap

On the other side of the political equation, the digital rights advocacy group Fight for the Future issued a statement saying the "framework reads like it was written by Sam Altman and Big Tech lobbyists. It's heavy on flowery language about 'innovation' and pathetic when it comes to substantive issues around discrimination, civil rights, and preventing AI-exacerbated harms. The framework eagerly suggests pouring Americans' tax dollars into AI research and development for military, defense, and private sector profiteering."

Meanwhile, the group said, "there's almost nothing meaningful around some of the most important and urgent AI policy issues like the technology's impact on policing, immigration, and worker's rights. There is no serious discussion of open source in the document, exposing a strong bias toward Big Tech dominance in the AI space. None of this is all that surprising given that companies like Clearview AI, Microsoft, and Amazon got far more air time during the process of creating this report than human rights groups and AI policy experts."

Fight for the Future said, "It seems that lawmakers in DC are less interested in regulating responsibly and more interested in rubbing elbows with CEOs and currying favor with those who stand to profit from unfettered AI. This roadmap leads to a dead end."

The statement said, "Fight for the Future will continue working with a broad coalition of groups fighting for meaningful regulation of AI that is rooted in human rights, free expression, and addressing the most immediate harms to the most marginalized people."

Schumer's bipartisan AI group releases 'roadmap' for legislation, including privacy protections

Posted May 15, 2024

Senate Majority Leader Charles Schumer's (D-NY) bipartisan working group on artificial intelligence has released its long-awaited report summarizing a series of closed-door strategy meetings last year and laying out a "roadmap" for legislation on safe uses and promoting the benefits of AI, including a call for long-stalled national data privacy protections.

Schumer's working group led by Sens. Mike Rounds (R-SD), Todd Young (R-IN) and Martin Heinrich (D-NM) released the "roadmap for artificial intelligence policy in the United States Senate" on May 15 summarizing the "insight forums" held last fall and winter with industry, civil rights and labor leaders, academics and others to guide Senate committees in drafting AI legislation.

"After talking to advocates, critics, academics, labor groups, civil rights leaders, stakeholders, developers, and more, our working group was able to identify key areas of policy that have bipartisan consensus," Schumer said in a statement announcing the new report.

"Now, the work continues with our Committees, Chairmen, and Ranking Members to develop and advance legislation with urgency and humility," he said.

Those legislative priorities include establishing "a strong comprehensive federal data privacy framework" as well as increased funding for research, boosting enforcement of existing laws, and encouraging "conscience consideration" of the impacts of AI on workers including "potential job displacement" and the need to "upskill and train workers," according to a summary of the report.

"Bolstering our national security by leading globally in the adoption of emerging technologies and addressing national security threats, risks, and opportunities for AI," is another legislative priority in the report.

And the bipartisan group is calling for legislation to address the "challenges posed by deepfakes related to election content and nonconsensual intimate images, as well as examining the impacts of AI on professional content creators and the journalism industry."

The highly touted report was released the same day that the Senate Rules Committee is slated to mark up several bipartisan bills for protecting elections from the growing threat of misinformation, including a proposal by Rules Chair Amy Klobuchar (D-MN) to ban the use of deceptive AI-generated content by campaigns and their allies.

The Schumer-backed report could provide a boost to efforts for quick passage of those proposals following a

committee vote. Schumer and Minority Leader Mitch McConnell (R-KY) are members of the Rules Committee.

Also noteworthy in the report is a call for a "comprehensive framework" for national privacy protections as the Senate Commerce Committee is considering a bipartisan proposal by Chair Maria Cantwell (D-WA) that would establish a first-time, cross-sector privacy law. The American Privacy Rights Act was introduced by Cantwell and House Energy and Commerce Chair Cathy McMorris Rodgers (R-WA) in April to preempt a growing patchwork of state requirements.

The House Energy and Commerce Committee approved a privacy bill under the chamber's last Democratic majority, but the legislation failed to gain final approval in part because of opposition by lawmakers from states with strong privacy protections such as California amid concerns about overriding those existing state-level controls.

The Senate bipartisan report appears to sidestep this lingering controversy by calling on committees to consider bolstering privacy protections for those sectors and areas under their jurisdiction as they consider broader AI legislation.

The Schumer group "encourages the relevant committees to consider whether there is a need for additional standards, or clarity around existing standards, to hold AI developers and deployers accountable if their products or actions cause harm to consumers, or to hold end users accountable if their actions cause harm, as well as how to enforce any such liability," the report says about a privacy framework.

"The AI Working Group encourages the relevant committees to explore policy mechanisms to reduce the prevalence of non-public personal information being stored in, or used by, AI systems, including providing appropriate incentives for research and development of privacy-enhancing technologies," according to the report.

And the report says the bipartisan AI working group "supports a strong comprehensive federal data privacy law to protect personal information. The legislation should address issues related to data minimization, data security, consumer data rights, consent and disclosure, and data brokers."

"As members of the AI Working Group, we are steadfast in our dedication to harnessing the full potential of AI while minimizing the risks of AI in the near and long term. We hope this roadmap will stimulate momentum for new and ongoing consideration of bipartisan AI legislation, ensure the United States remains at the forefront of innovation in this technology, and help all Americans benefit from the many opportunities created by AI," the report says.

"Given the cross-jurisdictional nature of AI policy issues, we encourage committees to continue to collaborate closely and frequently on AI legislation as well as agree on shared clear definitions for all key terms," says the report, highlighting the potential political challenges in moving on such a cross-cutting and omnipresent issue as the impact of emerging AI technologies.

"Finally, we encourage the executive branch to share with Congress, in a timely fashion and on an ongoing basis, updates on administration activities related to AI, including any AI-related Memorandums of Understanding with other countries and the results from any AI-related studies in order to better inform the legislative process," the report says.

Senate Intelligence Chair Warner presses AI companies on commitments to protect elections

Posted May 15, 2024

Senate Intelligence Chair Mark Warner (D-VA) is pressing major tech companies to prove that they are fulfilling their recent pledges to protect this year's elections from the growing threat of disinformation and deceptive AI-generated content.

"Against the backdrop of worldwide proliferation of malign influence activity globally — with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions," Warner wrote in May 14 letters to tech firms, asking them "about the specific measures your company is taking to implement" commitments made in February at the Munich Security Conference.

The letters were sent on the eve of a May 15 hearing by Warner's Intelligence Committee where National Intelligence Director Avril Haines and other security officials will testify on the government's efforts to counter foreign threats to the upcoming election.

Also, the Senate Rules Committee is slated on May 15 to mark up several bipartisan bills on securing the nation's election system including a proposal to ban deceptive AI-generated content by campaigns and their allies.

"While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy — and durability — of the initiatives and protection measures you adopt," Warner wrote in his letters to tech industry leaders.

His request for details by May 24 on what these companies are doing to mitigate the election risks of their products and services could be seen as an effort to assess whether legislation is needed.

"Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns," he wrote to stress the broader implications of those security measures for protecting the public online.

The letters were sent to 26 companies that signed the Tech Accord in Munich including Amazon, Anthropic,

GitHub, Google, IBM, Intuit, LinkedIn, McAfee, Microsoft, Meta, OpenAI, Stability AI, TikTok and X Corp., formerly Twitter.

"While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can — particularly in collaboration with civil society — dramatically shape the usage and wider impact of these technologies through proactive measures," Warner wrote to stress the importance of private-sector actions to protect elections.

Warner is asking the companies to report on steps they are taking "to attach content credentials, and other relevant provenance signals" to their products and services; "specific resources . . . your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public" about risks; "your company's engagement with candidates and election officials with respect to anticipating misuse of your products" and ways to effectively authenticate content and communicate that to the public, among other measures.

In anticipation of the Senate Rules Committee markup of election security legislation, the major tech industry group TechNet sent a letter to remind lawmakers of its recent comments to the Federal Election Commission arguing that current laws and rules should be applied to deceptive AI-generated content.

TechNet says it is urging the FEC "to clarify that the existing 'fraudulent misrepresentation' doctrine applies to deliberately deceptive AI-generated campaign content," according to the May 13 letter.

"We believe that candidates and their agents should be barred from utilizing AI to release deliberately misleading campaign content of any other candidate or political party," the tech industry group tells senators.

TechNet is reiterating its arguments that current rules can and should be applied to restricting the use of AI-generated content just as senators are poised to consider whether new laws are needed.

"We cannot wait. We are scheduling a markup of our bill. And we are going to have to work" to gain bipartisan support, Rules Chair Amy Klobuchar (D-MN) said last month when she announced her plans to bring up her election protection bill for a committee vote.

Colorado AI startups blast 'first-in-the-nation' state legislation as filled with loopholes

Posted May 15, 2024

Gov. Jared Polis (D) should veto the Colorado Artificial Intelligence Act as it could shield companies accused of algorithmic discrimination even as it is billed as consumer protection legislation, according to AI startups based in the state.

"The loopholes are big enough that you can drive a truck through it, and that is counter to what the goal is," said Kyle Shannon, founder of the video production platform Storyvine. "All of us here are absolutely for legislation to protect consumers ... it's just that this bill has a good title, but bad contents."

Shannon participated in a May 14 webinar held by the Chamber of Progress, a tech advocacy group for fairness and inclusion that discloses its partnership with Google and others, while asserting its independence from their influence in its decision-making. Shannon was joined by Kelly Kinnebrew, co-founder of the financial compliance company Minerva, and Logan Cerkovnik, founder of the open-source creatives platform Thumper.ai. The event was moderated by Kouri Marshall, the Chamber of Progress state and local public policy director.

The state legislation, if signed into law, is not set to take effect until February 2026, but opponents highlight its connection to "model" legislation being circulated to state legislators around the country by the HR giant Workday — which is being sued over algorithmic discrimination — and worry about how it could shape the course of national policy.

The bill is cited as making Colorado the first state in the country to broadly address artificial intelligence, but Cerkovnik said, "I don't think it serves Colorado and I think it may actually help embolden some of the lobbyists at the federal level, who would try to use this as an example to say, 'this is why we need our federal AI laws to preempt state laws, because state lawmakers can't do this well enough.'"

"We hope that by vetoing this bill, we could say, 'here's another chance for the Colorado legislature to take another whack at it,'" he said.

Cerkovnik said the bill's most glaring loophole has to do with what is considered "high risk" decision making as it exempts those where there's a human in the loop.

"The general gist," he said, "is if this is a decision support tool where the tool doesn't make the decision automatically, but it just says 'hey, make this decision and click *review* to save it,' that this is okay, that in these high-risk-of-discrimination areas, that that's allowed."

He said that's "a horrendous loophole to have in any algorithmic discrimination legislation. And I think the genesis of a lot of these problems in the legislation comes from the legislation being based off of Workday's model tech legislation text that they created and circulated back in the fall."

Cerkovnik also commented on the legislation's reliance on the National Institute of Standards and Technology's AI

Risk Management Framework, compliance with which — according to a summary of the bill provided by the legislature — would form an "affirmative defense" for a deployer or developer of covered AI systems. The bill also provides the same legal shield for using any "nationally or internationally recognized risk management framework for artificial intelligence systems that the bill or the attorney general designates," according to the summary.

The AI RMF is not itself a standard for implementing responsible AI — in fact, the NIST document notes such standards are badly needed — but outlines a process by which entities can examine their options and act according to their individual risk appetites.

A "choose-your-own-adventure regulatory framework doesn't make sense for anyone," Cerkovnik said. "The only reason the frameworks approach is chosen is because no one is really sure what they should be. The NIST framework cited as a default option itself hasn't reached a stable state. We need to wait to decide what we want as a framework before we move forward."

IBM urges Patent Office to adjust elements of guidance on AI-assisted inventions

Posted May 15, 2024

IBM Corp. is offering support for key aspects of the U.S. Patent and Trademark Office's guidance on "inventorship" and AI-assisted inventions while highlighting a handful of issues for USPTO to revisit, in comments on an initiative launched under President Biden's Oct. 30 executive order on AI.

IBM in its filing says it agrees with "three key points" in the guidance: "that AI-assisted inventions are not categorically unpatentable"; that the creation of an AI system "is not sufficient to establish inventorship of any invention developed using that same AI system"; and that U.S. statute and case law "require that an inventor be a natural person."

But the tech giant differs with USPTO on several issues, including legal interpretations, and seeks clarification on the guidance's scope and on compliance with its "duty of disclosure."

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

Among the 40-plus publicly posted comments, the Committee for Justice, a group that argues for limited government within constitutional constraints, said USPTO is on the right track and said a flexible definition of "human contributions" will fuel technological and societal advancements.

IBM in its comments emphasizes that AI is "incapable of invention" and takes issue with USPTO's language in the guidance stating that "an AI system — like other tools — may perform acts that, if performed by a human, could constitute inventorship."

"AI is indeed a powerful tool that can generate combinations of known elements in a highly productive manner to accelerate the pace of innovation. However, in the current state of the art, even the most sophisticated generative AI tools leverage models that utilize probabilities to derive output, not 'thinking,'" IBM says.

"Indeed, section 3(c) of the Executive Order under which the Guidance was promulgated defines an 'AI model' as a 'component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.' These tools are therefore similar to other tools used for assistance in the invention process in that they are incapable of conception, which as 'the complete performance of the mental part of the inventive act,' is the touchstone of inventorship."

The company says, "Case law has long recognized that while natural persons use such tools to derive combinations of elements, such tools are not capable of conception in and of themselves, but rather enable natural persons to conceive an invention."

IBM also raises concern with the USPTO guidance's reliance "on the factors set forth in *Pannu v. Iolab Corp.* to determine whether those contributions are 'significant' enough to constitute inventorship of an invention created with the assistance of AI and perhaps other tools incapable of conception."

The USPTO guidance released in February said "patent applications and patents for AI-assisted inventions must name the natural person(s) who significantly contributed to the invention as the inventor or joint inventors (i.e., meeting the *Pannu* factors as explained in section IV)," referring to a 1998 U.S. circuit court ruling in a patent infringement case.

USPTO said in Section IV of its guidance, "Courts have found that a failure to meet any one of these factors precludes that person from being named an inventor."

But IBM says in its filing, "While the *Pannu* factors have been applied to determine joint inventorship by natural persons, they have not been applied in the context of determining inventorship of tool-assisted inventions. Nor have they been applied in the context of sole inventorship. Instead, proper inventorship has long been determined by examining the contributions of natural persons to conception of the invention."

"Those determinations," IBM says, "have been and should continue to be made absent consideration of AI and other

tools used for assistance in the invention process that enable but are not capable of conception."

Further, IBM asks for a variety of clarifications, noting, for example, "The Office uses the terms 'AI systems,' 'other advanced systems,' and 'other tools' interchangeably throughout the Guidance. IBM asks for clarification, including definitions, to better understand the scope of the Guidance and help ensure compliance. IBM notes that the examples appear to be limited to use of generative AI and a deep neural network (DNN)-based prediction model for assistance in the invention process."

And, on duty of disclosure, IBM "respectfully requests that the Office provide additional examples of what is and could be considered material information in the AI context as well as example submissions to the Office disclosing that information because failure to comply with the duty of disclosure heightens the risk of unenforceability."

"IBM also asks the Office to clarify whether each individual associated with the filing and prosecution of a patent application must submit evidence of the type described in the example and any additional examples to the Office for pending patent applications," the company says. "Doing so can be a challenge for applicants because records on use of AI during the invention process may no longer exist for those applications."

FTC warns of potential liability for feeding connected-car data into algorithms

Posted May 15, 2024

The Federal Trade Commission, in its latest warning on how uses of artificial intelligence could run afoul of existing laws, says using data collected by connected cars in automated decision-making processes may violate legal protections related to sensitive consumer data.

"Car manufacturers — and all businesses — should take note that the FTC will take action to protect consumers against the illegal collection, use, and disclosure of their personal data. Recent enforcement actions illustrate this point," according to a May 14 FTC blog post. It was prepared by the FTC Office of Technology and Division of Privacy and Identity Protection.

The intertwined issues of connected cars, data uses and security, and artificial intelligence have grabbed attention on Capitol Hill and within the executive branch.

The Commerce Department's Bureau of Industry and Security in March issued an advance notice of proposed rulemaking on security of connected vehicles, with a focus on threats from foreign adversaries. The comment deadline was April 30.

Senate Banking Chairman Sherrod Brown (D-OH) submitted a comment urging Commerce to move ahead with a rulemaking banning the import of Chinese-made connected vehicles that could transmit sensitive data back to China and pose both cybersecurity and artificial intelligence-related national security risks.

The FTC in its blog post says, "Some say the car a person drives can say a lot about them. As cars get 'connected,' this turns out to be truer than many people might have realized. While connectivity can let drivers do things like play their favorite internet radio stations or unlock their car with an app, connected cars can also collect a lot of data about people."

The blog post says, "This data could be sensitive — such as biometric information or location — and its collection, use, and disclosure can threaten consumers' privacy and financial welfare."

"Connected cars have been on the FTC's radar for years," according to the blog post, which goes on to say, "Over the years, privacy advocates have raised concerns about the vast amount of data that could be collected from cars, such as biometric, telematic, geolocation, video, and other personal information. News reports have also suggested that data from connected cars could be used to stalk people or affect their insurance rates."

The FTC touches on potentially AI-related issues, saying, "Many have noted that when any company collects a large amount of sensitive data, it can pose national security issues if that data is shared with foreign actors."

The FTC points out that "Geolocation data is sensitive and subject to enhanced protections under the FTC Act," explaining, "In a series of seminal cases in recent years, the Commission has established that the collection, use, and disclosure of location can be an unfair practice."

It also says, "Surreptitious disclosure of sensitive information can be an unfair practice."

"Companies that have legitimate access to consumers' sensitive information must ensure that the data is used only for the reasons they collected that information," the FTC stresses.

And finally, the blog post specifically takes on AI, saying, "Using sensitive data for automated decisions can also be unlawful."

"Companies that feed consumer data into algorithms may be liable for harmful automated decisions," the blog post says. "The FTC recently took action against Rite Aid, saying in a complaint that the company enrolled people into a facial recognition program that alerted employees when suspected matches entered their stores."

"The complaint includes allegations that Rite Aid failed to take reasonable steps to prevent low-quality images from

being used with the program, increasing the likelihood of false-positive match alerts. In some cases, false alerts came with recommended actions, such as removing people from the store or calling the police, and employees followed through on those recommendations."

"As a result of the FTC's action," the blog post says, "Rite Aid agreed to a 5-year ban on the use of facial recognition technology."

House Armed Services' draft defense policy bill calls for review of Pentagon AI spending

Posted May 14, 2024

The House Armed Services Committee unveiled draft fiscal 2025 defense authorization legislation this week that includes provisions requiring the Pentagon to audit and report its spending on artificial intelligence, with lawmakers expressing concern about the data used to train these AI models.

"The committee is concerned about accurate budgeting for inclusion" of AI, machine learning and computer vision into Pentagon programs, says the draft legislation released May 13. The full committee is scheduled to debate the "chairman's mark" bill on May 22.

"Therefore, the committee directs the Secretary of Defense, in coordination with the Undersecretary of Defense for Acquisition and Sustainment, to report to the House Committee on Armed Services by March 1, 2025, with a plan to ensure the budgeting process for programs containing AI elements such as ML and CV, include estimates for the data required to train, maintain and improve AI models or systems," the bill says.

The report must include "(1) an assessment of the costs associated with the data required to train, maintain or improve AI models or systems; (2) an assessment of the current programs containing AI elements; and (3) a process to ensure the costs associated with the data required to train, maintain or improve AI models or systems are appropriately incorporated into life cycle sustainment estimates for future programs containing Artificial Intelligence elements," according to the draft committee bill.

The draft National Defense Authorization Act is intended to implement President Biden's $850 billion budget proposal released in March for Defense Department discretionary spending in fiscal 2025.

A separate draft plan released by the Armed Services cyber, IT and innovation subcommittee includes provisions for DOD to develop a strategy on preparing the massive amounts of data generated by the military for use by AI technologies, with s focus on encouraging seamless integration across military operations.

The data management strategy required of the Secretary of Defense within 270 days must include the "activities of the Chief Digital and Artificial Intelligence Officer of the Department of Defense to increase and synchronize the use of modern data formats and modern data sharing standards across the Department of Defense, including the Armed Forces in the Department of Defense," according to the section on "usability of antiquated data" in the subcommittee draft bill.

"The activities of the military departments to increase the use of modern data formats and modern data sharing standards for command and control systems, weapon systems, and sensors associated with such weapon systems," must also be included in the strategy, the bill says.

The strategy should include an "identification of barriers to the use of modern data formats and modern data sharing standards within weapon systems and sensors associated with such weapon systems across the Department of Defense, including the Armed Forces in the Department of Defense," the bill adds.

Also, the subcommittee plan calls on DOD to develop a secure system for the use of biological data for training AI models.

"This section would require the Under Secretary of Defense for Research and Engineering, in coordination with the Chief Digital and Artificial Intelligence Officer, to submit an implementation plan, not later than 1 year after the date of the enactment of this Act, on the feasibility of establishing a secure computing and data storage environment to facilitate the testing of artificial intelligence models trained on biological data and the development and testing of products generated by such models," the draft legislation says.