SENATE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

"Oversight of AI: Legislating on Artificial Intelligence"

September 12, 2023 – 2:30 PM

OVERVIEW

On Tuesday, September 12, the Senate Judiciary Subcommittee on Privacy, Technology, and the Law held a hearing entitled, "Oversight of AI: Legislating on Artificial Intelligence." During the hearing, Senators and witnesses discussed oversight and accountability, content authentication and moderation, children's safety, national security, workforce impacts, and competition and intellectual property protections.

OPENING STATEMENTS

- Chair Richard Blumenthal (D-CT)
- Ranking Member Josh Hawley (R-MO)

WITNESS PANEL

- Dr. William Dally – Chief Scientist and Senior Vice President of Research, NVIDIA Corporation
- Mr. Brad Smith – Vice Chair and President, Microsoft Corporation
- Dr. Woodrow Hartzog – Professor of Law, Boston University School of Law; Fellow, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis

QUESTION AND ANSWER SUMMARY

Oversight and Accountability

Chair Blumenthal asked how to safeguard against the downsides of AI, including discrimination or surveillance, and if a licensing regime and oversight entity would be sufficient. Mr. Smith agreed a licensing regime is a strong start, especially for frontier models and the most high-risk applications, but warned it will not be sufficient alone. He also noted it would be a mistake to assume one single agency or regime could be effective for all applications; instead, he suggested ensuring all government agencies master the ability to assess AI. Chair Blumenthal agreed AI will be used in a variety of cross-sector applications, so a broad, government-wide understanding is needed, but argued a single oversight entity is crucial to support effective harm reduction.

Chair Blumenthal asked how to ensure fears of uncontrollable, autonomous AI, which Dr. Dally characterized as science fiction in his opening testimony, are not realized in the future. Dr. Dally clarified uncontrollable artificial general intelligence should be regarded as science fiction, not autonomous systems more broadly. To ensure AI remains controlled, he stressed the importance of human engagement with AI for every critical application, closely monitoring the system inputs to prevent any harmful outputs.

Sen. Amy Klobuchar (D-MN) noted the White House announced eight additional companies joined voluntary commitments to advance safe, secure, and transparent AI development, including Nvidia, and asked about the steps Nvidia has taken to ensure the responsible use of AI. Dr. Dally highlighted the Nemo Guardrails program, which includes safety controls for Nvidia's large language model (LLM) Nemo to prevent the generation of offensive outputs. He added Nvidia has guidance for all internal models and their use, provides the details on where models originated and what data they are trained on, and tests all models thoroughly for bias and safety.

Sen. Klobuchar asked if Congress should prioritize regulations on the inputs and design of AI systems, rather than outputs and capabilities. Professor Hartzog advocated for regulations on both inputs and outputs, but recognized inputs and design have been ignored in recent discussions on regulatory options.

Sen. Marsha Blackburn (R-TN) asked how to prevent the use of AI for surveillance purposes. Professor Hartzog argued facial recognition technologies in certain applications of biometric surveillance are fundamentally dangerous and should be banned outright. Dr. Dally added technology companies must be very careful to ensure their products are only sold for good commercial purposes, and not to oppress people.

Sen. Jon Ossoff (D-GA) asked how to define the scope of an AI-focused legislative framework, including the technologies, services, and products subject to regulation. Mr. Smith cited three layers of technology to focus regulations on: first, the most powerful frontier or foundation AI models; second, the high-risk applications and deployments of AI, such as those that could impact privacy or civil liberties; and third, data center infrastructure, ensuring AI applications are deployed securely.

Sen. Ossoff raised concerns as more models are trained and developed, there may be a proliferation of less sophisticated models that could be used to cause significant harms. He asked what threshold of power should define the scope of regulative capabilities. Mr. Smith argued this is a critical question many industry stakeholders are working to answer, particularly how to solve for the future proliferation of open-source models with effective safety controls. He added identifying the threshold for a license requirement is partly why establishing a licensing regime may prove difficult; it is important to ensure licenses are not so hard to attain that only a small number of major companies can get them. Sen. Ossoff asked who the licensed entity for AI should be. Mr. Smith argued the developer of certain AI models should be required to get a license to sell that model only after it has been certified safe. He added disclosure requirements could also be incorporated for certain training processes, depending on the proposed application of the model, governed by an independent oversight body. To establish an effective safety standard for AI models, Mr. Smith suggested bringing together common industry standards, federal regulation, and international standards. Dr. Dally recommended balancing efforts to examine and mitigate risks posed by AI models and ensuring the U.S. does not cede global leadership in AI development as regulators consider defining a licensing regime. He added the threshold for a license requirement should depend on its application, noting a model used for medical diagnostics poses a higher risk compared to one used to control the temperature of a building, for example.

Sen. Ossoff asked how regulations can work without international law, given the borderless nature of this type of digital technology. Professor Hartzog argued there will be limits to controlling AI, even with international cooperation. He warned monitoring the entire scope of global AI activities would require deploying a dangerous level of surveillance, raising separate privacy concerns. Mr. Smith agreed there is a need for international coordination, which he argued will more likely come from like-minded governments than a global governance system. Dr. Dally explained the deployment and use of an AI model will be easier to effectively regulate than the creation of one, particularly in an international context.

Content Authentication and Moderation

Sen. Klobuchar asked why the health of democracy and meaningful civil discourse would benefit from initiatives to help protect against deception or fraud facilitated by AI-generated content, as Mr. Smith argued in his opening testimony. Mr. Smith contended regulations on AI should include several key principles: first, consumers should have the right to know whether the content they view is AI-generated; and second, lawmakers should establish a provenance system to label legitimate content so it cannot be easily altered to create a deepfake. He advocated for a collective effort from the industry and government to establish consensus on how to address deepfakes and identify legitimate content.

Sen. Klobuchar raised concerns about the impact of AI-generated content on elections and asked if Congress should ban certain types of misleading AI conduct related to federal candidates and campaign ads. Professor Hartzog argued bright-line rules and prohibitions on deceptive ads are critical, keeping in mind free expression and constitutional protections. He warned that procedural measures often give the illusion of protection without making any meaningful impact on the harmful conduct; instead, he suggested considering how to prohibit both deceptive and abusive practices, leveraging existing laws that regulate abusive trade practices.

Sen. Klobuchar asked about private sector efforts to prevent the use of AI for criminal purposes. Dr. Dally argued the use of provenance and authentication systems to validate legitimate content are the best measures against deepfakes, combined with the use of watermarks to identify generated content and public education campaigns to ensure people understand the technology's capabilities and how to guard against them.

Sen. Mazie Hirono (D-HI) raised concerns about the use of AI to spread disinformation and sow distrust in the federal government during a natural disaster. She asked how lawmakers can help prevent foreign entities from disseminating disinformation to vulnerable populations. Mr. Smith suggested using AI to detect malicious activities, noting the technology can accelerate the speed of mitigation efforts. He also emphasized the need for the U.S. to take a strong stance, alongside international partners, against foreign adversaries and establish global standards on unacceptable conduct. Sen. Hirono asked how to both identify the malicious conduct and alert citizens of the issue. Mr. Smith argued private companies like Microsoft must support detection efforts, given their vast data and expertise. He also urged lawmakers to establish a bipartisan framework that facilitates information sharing between private and public entities.

Sen. John Kennedy (R-LA) asked if consumers should have the right to know if the content they view is generated by AI. Dr. Dally and Mr. Smith expressed support for general disclosure requirements. Mr. Smith noted, however, certain written contexts may be more complex to regulate, as AI can often be used to help draft reports or speeches, involving more human engagement. Professor Hartzog advocated for disclosures in contexts where consumers do not expect to engage with AI. Sen. Kennedy asked if consumers are entitled to know who owns the AI model and where generated content originated when they engage with AI-generated content. Dr. Dally argued it depends on the context; disclosures on who generated content for political purposes, for example, could be beneficial. Mr. Smith generally supported broad disclosures about who owns the program generating content, but recognized there are circumstances where anonymous speech should be preserved.

Chair Blumenthal noted he is particularly focused on election interference as the 2024 election cycle approaches and questioned how to best balance the need to protect elections without harming free expression. Dr. Dally agreed misleading content is a grave concern and echoed calls for provenance mechanisms to identify real content and watermarks to disclose generated content. He recognized while it is important to protect against election interference, AI-generated content still qualifies as speech; banning content could create a dangerous precedent, so disclosure requirements should be prioritized instead. Mr. Smith agreed First Amendment protections should remain a key priority, but asserted the Russian government does not qualify for these protections and urged the federal government to take a strong stance on how to mitigate foreign interference. He cautioned against removing content entirely, as that could overstep free speech protections, and instead suggested efforts to relabel harmful content. Professor Hartzog shared concerns about banning certain speech, alongside skepticism about the effectiveness of disclosures alone.

Children's Safety

Ranking Member Hawley asked about Microsoft's efforts to protect children online, including whether kids can use Bing Chat. Mr. Smith noted there are certain age controls in place, but confirmed kids can register to use the product over a certain age. Ranking Member Hawley inquired about Microsoft's age verification process. Mr. Smith explained Microsoft deploys age verification systems, typically parental consent mechanisms, across several different products, including gaming.

Ranking Member Hawley asked what happens to the information collected on children when they interact with Bing Chat. Mr. Smith asserted Microsoft protects the privacy of children, adhering to the Children's Online Privacy Protection Act (COPPA) rules on the use and retention of children's data. In addition to protecting privacy, he explained Microsoft is hyper-focused on ensuring children are not able to use products like Bing Chat

in ways that would cause harms to themselves or others. Mr. Smith highlighted the models' safety architecture, which includes controls to flag harmful questions and intervene to prevent providing an answer; mental health assistance would be provided in response to a question about self-harm, for example.

Ranking Member Hawley asked where children's data is stored by Microsoft, and who has access to the data. Mr. Smith explained any data collected on an American user is stored in the United States, and the users themselves would have access to it. He asserted Microsoft believes individuals should have the right to find out what information is collected on them, to correct it if necessary, or to delete it upon request. Ranking Member Hawley raised concerns about data storage and access issues in the social media industry more broadly, and whether children's data could be accessed in China.

Ranking Member Hawley argued a 13-year-old is too young to engage with AI chatbots. He asked if Microsoft would commit to raising its age limit for Bing Chat and implementing a stronger age verification mechanism. Mr. Smith committed to considering the issue. He explained there are many helpful applications of an AI chatbot for kids of different ages, assuming it is used in a safe, controlled manner; for example, he highlighted the value of an AI tutor in an educational context. Ranking Member Hawley raised concerns Microsoft's safety architecture did not protect adults, citing reports of an incident where the chatbot encouraged a user to end his marriage. Mr. Smith explained the incident occurred at the very early stages of the program, and the user engaged in a way Microsoft did not anticipate; once the issue was detected, it was fixed immediately. Ranking Member Hawley questioned if Microsoft has envisioned all of the questions a 13-year-old might ask Bing Chat. Mr. Smith argued AI developers will have an increasing opportunity to learn from past mistakes and improve models. Ranking Member Hawley asserted past failures to protect children cannot be used to improve future models. Mr. Smith agreed no users – children or adults – should be used as experiments for technological development, but acknowledged technology requires real users to advance, and because AI accelerates at such a fast rate, issues can be fixed within hours and days. Ranking Member Hawley opposed retroactive fixes, as well as the concept consumers should simply trust private companies to implement effective safety mechanisms. Mr. Smith argued while Microsoft works every day to earn consumer trust, a licensing obligation should be implemented to ensure accountability, as outlined in Ranking Member Hawley and Chair Blumenthal's framework for AI regulation.

National Security

Sen. Blackburn raised concerns about Chinese Communist Party (CCP) disinformation and influence campaigns against U.S. citizens, citing Microsoft's recent report issued about the campaigns. She asked how the technology industry can help combat these efforts from the CCP. Mr. Smith argued companies should work to ensure their products are not used by foreign governments in this manner. He added there is room for additional export control considerations, as well as Know-Your-Customer (KYC) requirements; these requirements could help ensure companies are better aware of product misuse. Further, Mr. Smith advocated for the use of AI in a defensive context, including using AI to detect suspicious patterns of communication. He argued Microsoft seeks to be a leading voice alongside industry partners in calling for a higher standard, ensuring their technologies are not used to interfere in other countries, particularly elections.

Sen. Blackburn asked if Microsoft examined other countries besides China in its report on disinformation campaigns. Mr. Smith explained the report focused on East Asia, where Microsoft identified prolific activities from China, Iran, and most actively Russia. He reported the Russian government spends an estimated $1 billion a year on cyber influence operations, ultimately aiming to undermine public confidence in the U.S., the South Pacific, and across Africa. Mr. Smith asserted this is a significant problem that requires stronger action to counter, such as a Know-Your-Cloud requirement to ensure systems are deployed in secure data centers.

Ranking Member Hawley argued China poses the most significant national security threat to the U.S. He questioned if Microsoft is concerned about its degree of entwinement with China, and if the company should consider decoupling to ensure U.S. national security interests are not compromised. Mr. Smith agreed Microsoft should remain closely focused on this issue, but noted to some degree, Microsoft is the alma mater of the technology leaders in every country, not just China. He argued the company needs to have very specific controls on who uses its technology, for what, and how; this is why, for example, Microsoft does not work on quantum computing, does not provide facial recognition services, and does not focus on synthetic media. He added it is important Microsoft runs its services in a U.S.-based data center, rather than a Chinese company's data center.

Ranking Member Hawley argued while Microsoft may be the alma mater of many companies, China is unique in its concerning surveillance activities. He questioned why Microsoft would want to remain involved in this issue. Mr. Smith asserted Microsoft is not involved, nor does it want to be.

Ranking Member Hawley asked if Microsoft would close its centers in China. Mr. Smith contended closing those centers would not accomplish the security goals under consideration. He recognized China's surveillance activities are a significant problem, but refuted any allegations Microsoft operates a revolving door of individuals flowing from its Chinese centers to the Chinese government. He condemned the Chinese government's harmful surveillance efforts and asserted Microsoft does everything possible to ensure its technology is not used for these activities in China or globally.

Ranking Member Hawley asked about the safeguards in place to prevent the misuse of Microsoft's technology. Mr. Smith explained the company has very tight controls to limit the use of facial recognition technology in China, making it very difficult to use it for any real-time surveillance. He noted, however, while the U.S. is a leader in many AI fields, China leads in facial recognition technology development. Ranking Member Hawley asked how much money Microsoft has invested in AI development in China. Mr. Smith reported the revenue made in China makes up approximately 1.5 percent of Microsoft's global revenue. Ranking Member Hawley then inferred Microsoft could afford to decouple. Mr. Smith contended decoupling is not the right strategy.

Chair Blumenthal questioned if Microsoft is satisfied with the protections implemented to counter China's misuse of its technologies. Mr. Smith applauded Microsoft's track record and vigilance about the services it offers and how they are used. He advocated for a broader conversation about export controls, noting the U.S. leads globally in GPU chips, cloud infrastructure, and foundation models and must ensure they are used properly. Chair Blumenthal asked how to draw a line on the hardware U.S. technology companies should be allowed to provide other nations. Dr. Dally argued there is a careful balance to be made between restricting certain uses of U.S. chips and disadvantaging U.S. companies. He warned there are many other international chip production companies, and if people cannot get them from an American company, they will just go to someone else; as a result, developers will prioritize creating software for competitors, rather than American companies. He urged lawmakers to carefully balance the national security implications with preserving U.S. leadership.

Workforce Impacts

Sen. Hirono asked which jobs are most at risk of being lost to AI. Mr. Smith inferred jobs in the service industry, such as drive-through attendants, could be the first to be eliminated, as they involve limited human engagement. He argued, however, that automating certain routine positions could free up opportunities for more creative paths.

Ranking Member Hawley raised concerns about the loss of certain jobs to AI, regardless of their creative capacity, opposing the concept of diminishing the value of working-class jobs. Mr. Smith clarified he believes those jobs will be impacted by AI, but did not imply it was a positive or negative effect. He noted automation has impacted many jobs over the last 200 years, and adjusting to these impacts is an ongoing consideration as technology advances. He argued the question is how to ensure technology advances in a way that broadens economic opportunity, rather than narrowing it. Mr. Smith raised concerns the economic divide has continued to widen in recent decades, leaving those who have less education with a lower income level, and asserted the broader goal should be identifying how to use AI to advance productivity and income for a larger range of people.

Chair Blumenthal emphasized the need to retrain the workforce to ensure workers are prepared to engage with emerging technologies. He noted AI presents tremendous opportunities across sectors for many different types of roles, but raised concerns about existing labor shortages, noting this may be the largest challenge facing the American economy. Mr. Smith explained the world is currently experiencing a massive demographic shift with a decline in the working-age population. He suggested AI could be an important tool to solve some of these labor shortages, particularly in contexts like call centers that could become more automated, alongside efforts to upskill workers. Mr. Smith expressed optimism that AI presents exciting opportunities to leverage human intelligence and raise wages for workers.

Competition and Intellectual Property Protections

Sen. Klobuchar raised concerns some AI platforms use local news content without compensation to train AI models, and noted the Journalism Competition and Preservation Act (S.1094) would allow local news organizations to negotiate with these platforms. She asked about the impacts of AI on local journalism. Mr. Smith highlighted three concerns: first, local news is fundamental to the health of the country, and efforts to preserve and promote it are essential; second, local organizations should be allowed to decide whether their content can be used to train models, and should be able to negotiate collectively; and third, AI can be used to help local journalists and supporting this application should remain a priority for companies and regulators.

Sen. Klobuchar noted Nvidia announced a partnership with Getty Images in March to develop models that generate new images, providing royalties to content creators. She asked about the importance of compensating creators for their work when developing generative AI models. Dr. Dally explained Nvidia believes in the protection of individuals' intellectual property (IP) rights and partnered with Getty to train their Picasso model and ensure creators are compensated for their content. He argued people who provide IP to train models should benefit from the use of that IP.

--

Please click here for the archived hearing.