BEN RAY LUJÁN
NEW MEXICO
498 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-6621

United States Senate
WASHINGTON, DC 20510-3105

COMMITTEES:
COMMERCE, SCIENCE, AND TRANSPORTATION
CHAIR, COMMUNICATIONS, MEDIA, AND BROADBAND
AGRICULTURE, NUTRITION, AND FORESTRY
HEALTH, EDUCATION, LABOR, AND PENSIONS
INDIAN AFFAIRS
BUDGET

June 12, 2023

The Honorable Alan Davidson
Administrator
National Telecommunications and Information Administration
1401 Constitution Avenue NW
Washington, DC 20230

RE: National Telecommunications and Information Administration Request for Comment on Artificial Intelligence (AI) Accountability (Docket No. 230407-0093)

Dear Administrator Davidson,

I applaud your commitment to accountable and trustworthy artificial intelligence systems (AI). AI is a critical technology that stands to transform all aspects of society. It is time for Congress and the Administration to create and implement responsible guardrails around AI development, governance, and use. As Chair of the Subcommittee on Communications, Media, and Broadband and member of the Consumer Protection and Science Subcommittees under the Senate Committee on Commerce, Science, and Transportation, I want to ensure online platforms that use AI models or offer them for consumer use are doing so in a responsible way.

In particular, audits or certifications of AI must include transparency, disclosure requirements, and tools to assess and incentivize language equity and protections for artists and consumers.

Language Equity

Any certification, audits, or assessments of artificial intelligence systems must include requirements that the AI performs consistently across languages. There are well-known cross-sector biases in AI systems with respect to race,[1] gender,[2] and other characteristics. With the recent explosion of large language models, language equity is an increasingly important issue that developers and auditors of AI must assess prior to making a model available for commercial or consumer use. Large language models likely do not work as well in low-resourced languages in which there is less high-quality training data,[3] leading to widespread misinformation, disinformation, scams, and fraud amongst immigrant communities.[4]

I introduced the Language-inclusive Support and Transparency for Online Services (LISTOS) Act to improve multilingual large language models, automated decision-making systems, and content moderation practices online to better protect non-English speaking communities. To enhance and cement these protections, I urge you to incorporate language equity and

[1] "These robots were trained on AI. They became racist and sexist.", Pranshu Verma, The Washington Post, July 16, 2022, https://www.washingtonpost.com/technology/2022/07/16/racist-robots-ai/
[2] "'There is no standard': investigation finds AI algorithms objectify women's bodies", Gianluca Mauro and Hilke Schellmann, The Guardian, February 8, 2023, https://www.theguardian.com/technology/2023/feb/08/biased-ai-algorithms-racy-women-bodies
[3] "Lost in Translation – Lange Language Models in Non-English Content Analysis", Gabriel Nicholas and Aliya Bhatia, Center for Democracy and Technology, May 2023, https://cdt.org/wp-content/uploads/2023/05/non-en-content-analysis-primer-051223-1203.pdf
[4] "Misinformation Swirls in Non-English Languages Ahead of Midterms", Tiffany Hsu, New York Times, October 12,2022, https://www.nytimes.com/2022/10/12/business/media/midterms-foreign-language-misinformation.html

BEN RAY LUJÁN
NEW MEXICO
498 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-6621

United States Senate
WASHINGTON, DC 20510-3105

COMMITTEES:
COMMERCE, SCIENCE, AND TRANSPORTATION
CHAIR, COMMUNICATIONS, MEDIA, AND BROADBAND
AGRICULTURE, NUTRITION, AND FORESTRY
HEALTH, EDUCATION, LABOR, AND PENSIONS
INDIAN AFFAIRS
BUDGET

investment questions and requirements in any and all recommendations for audits, assessments, or certifications of AI systems.

Protections for Artists

Powerful generative AI models can create extremely convincing text, images, and audio, making it a powerful tool for not only creators and consumers, but also for fraudsters and scammers. Creative industries, especially music and visual arts, are very concerned about copyright infringement and subsequent market dilution.[5] OpenAI has openly acknowledged that its programs are trained on "large, publicly available datasets that include copyrighted works."[6] Creating such copies without permission from copyright owners may infringe copyright, and powerful AI models can easily create sound, images, or videos that are indistinguishable from artists' own voice, name, image, or likeness.

I urge you to include questions and tools in audits of AI that protect artists. These protections should include existing copyright protections, but also recommendations related to how model developers of AI and users can appropriately credit and compensate artists when (1) their art is used to train AI models, or (2) AI-generated outputs are created that "in the style of" artists, leading to name, image, likeness issues or market dilution.

Consumer Protections

Generative AI enables the creation of false content quickly, cheaply, and at scale. AI-generated images and voices are already extremely realistic, sometimes indistinguishable from the real thing, and AI-generated video quality is rapidly improving. AI-generated photos are flooding social media and the internet and are being used to spread false narratives.[7] Scammers are using generative AI to clone individuals' voices and use those fake recordings to scam family members,[8] a problem so widespread that the FTC recently put out a consumer alert on the issue.[9]

Assessments of AI must pay particular attention to models that can generate content and the intended use cases for those models. I urge you to include questions regarding what types of guardrails AI model developers include in their products to track or prevent users from contributing to fraudulent, false or misleading information related to elections, civil rights or public health, harassing or abusive content, or to clone individuals' voices or likenesses. For example, do model developers include watermarks in their AI-generated content to provide

[5] "Music Executives Grapple with Generative AI on Earnings Calls", Ashley Carman, Bloomberg News, April 27, 2023, https://www.bloomberg.com/news/newsletters/2023-04-27/music-executives-grapple-with-generative-ai-on-earnings-calls
[6] Comment Regarding Request for Comment on Intellectual Property Protection for Artificial Intelligence Innovation, Comment of OpenAI, USPTO, https://www.uspto.gov/sites/default/files/documents/OpenAI_RFC-84-FR-58141.pdf
[7] "That photo of Trump being tackled by police isn't what you this it is as the internet enters a new era of AI disinformation", Arijeta Lajka and Philip Marcelo, The Associated Press, March 23, 2013, the https://fortune.com/2023/03/23/a-i-generated-photo-video-disinformation-internet/
[8] "Scammers use AI to clone woman's voice, terrify family with fake ransom call", Bailee Hill, Fox News, April 18, 2023, https://www.foxnews.com/media/scammers-ai-clone-womans-voice-terrify-family-fake-ransom-call-worst-day-life
[9] "Scammers use AI to enhance their family emergency schemes", Alvaro Puig, Consumer Alerts, Federal Trade Commission, March 20, 2023, https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes

BEN RAY LUJÁN
NEW MEXICO
498 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-6621

United States Senate
WASHINGTON, DC 20510-3105

COMMITTEES:
COMMERCE, SCIENCE, AND TRANSPORTATION
CHAIR, COMMUNICATIONS, MEDIA, AND BROADBAND
AGRICULTURE, NUTRITION, AND FORESTRY
HEALTH, EDUCATION, LABOR, AND PENSIONS
INDIAN AFFAIRS
BUDGET

some form of evidence that the content was AI-generated? Do they include enforceable terms and conditions in generative AI products to prohibit these types of uses?

Privacy

AI poses the same privacy questions as social media and the internet age with increasing urgency. Large AI models are trained using vast amounts of data, much of which is scraped from the internet with no regard for data privacy.[10] Further, there are no standard documentation requirements relating to data sourcing and sensitive information that might be found in datasets, making it difficult to ascertain just how much sensitive or personally identifiable data is in AI models and what might be accidentally revealed. The data users input into consumer-facing AI models like chatbots are also rife for privacy breaches – a ChatGPT leak in March revealed users' personal and financial data.[11] Tech companies themselves have banned the use of ChatGPT by employees due to fears that OpenAI would access and use sensitive company information input into the chatbot.[12]

Audits and assessments of AI tools must ensure privacy protections. Methods of detecting and masking sensitive and personally-identifiable data, both in training datasets and data input by users after model release, should be a core part of any AI model. AI model developers should also be required to enforce a "right to be forgotten" and provide avenues for individuals and users to request and verify deletions of sensitive and private data.

A responsible AI framework is critical to ensuring that this rapidly advancing technology is used in ways that promote digital equity, creativity, democratic integrity, and economic equity. I urge you to use this well-timed and thoughtful docket to support the creation of responsible AI frameworks and principles.

Sincerely,

Ben Ray Luján
United States Senator

[10] "ChatGPT is a data privacy nightmare, and we ought to be concerned", Uri Gal, Ars Technica, February 8, 2023, https://arstechnica.com/information-technology/2023/02/chatgpt-is-a-data-privacy-nightmare-and-you-ought-to-be-concerned/
[11] "March 20 ChatGPT outage: Here's what happened", OpenAI, March 24, 2023, https://openai.com/blog/march-20-chatgpt-outage
[12] "Big Tech is already warning us about AI privacy problems", Elizabeth Lopatto, The Verge, May 19, 2023, https://www.theverge.com/2023/5/19/23730037/openai-ban-apple-banks-privacy