STATEMENT BY
JOHN BRENNAN, Ph.D.
GENERAL MANAGER, PUBLIC SECTOR
SCALE AI

BEFORE THE
SUBCOMMITTEE ON THE COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET
OF THE
HOUSE JUDICIARY COMMITTEE

ENTITLED
“IP AND STRATEGIC COMPETITION WITH CHINA: IP THEFT, CYBERSECURITY, AND AI”

SEPTEMBER 20, 2023

Chairman Issa, Ranking Member Johnson, and Members of the Subcommittee on the Courts, Intellectual Property and the Internet, thank you for the opportunity to be here today to testify on the importance of U.S. leadership in the development and adoption of responsible, ethical artificial intelligence (AI).

I am honored to be here today to discuss these topics with you.

**INTRODUCTION**

My name is John Brennan, and I joined Scale AI (Scale) in April to lead our public sector business. This work enables me to be on the front lines of the intersection between AI development, government adoption, and its proper governance structure.

Supporting the federal government is deeply personal to me as I come from a family with four generations of service to our nation. From my childhood growing up in Mobile, Alabama, to my time at West Point, and throughout my professional career in the military and intelligence community, where I was humbled to serve my family's 100th year of service, I have always felt a strong commitment to ensuring the United States leads the world in the adoption of next generation technologies in support of our democratic values.

Scale was founded in 2016 with the mission of accelerating the development of AI. From our earliest days labeling data for autonomous vehicle programs at companies like General Motors and Toyota, to our commercial work today with the leading frontier model developers like OpenAI, Microsoft and Meta, and our work with federal government stakeholders, like the Department of Defense's (DoD) Chief Digital and AI Office (CDAO) and U.S. Army, Scale has always been on the forefront of AI development.

Today, Scale fine-tunes, red teams, or tests and evaluates nearly all of the leading frontier large language models (LLMs), which provides us a unique vantage point to best understand the development of safe, secure, and trustworthy AI.

**AI SUPERIORITY IS CRITICAL TO U.S. GLOBAL LEADERSHIP**

While AI may be more accessible today through LLMs, this does not mean that the technology is new. The truth is that AI has been around for decades and is already heavily in use in the U.S. and countries around the world. From the development of the Turing test,[1] to machine learning computer vision algorithms helping automobiles improve their safety and even streaming services suggesting new programs for consumers to watch,[2] machine learning and AI have been in use for decades.

These years of experience have enabled countries around the world to understand how to embrace AI in line with their values and begin crafting a governance framework around them. At a fundamental level, generative AI models learn patterns and structure from large datasets to create new content, and the algorithms and their outputs reflect the values and biases of the information that they are trained on. This is why it is critical that AI is developed and trained in alignment with democratic values. If the U.S. does not continue to heavily invest in maintaining our leadership in the development and adoption of generative AI, we risk letting the ideals of the Chinese government drive AI development around the world.

China is investing disproportionately in AI and has also started to craft its own governance framework that requires AI to adhere to communist party principles.[3] It is clear that China is leveraging the combined influence of government and industry (military-civil fusion), along with distinct IP and cybersecurity rules that favor state control of technology, to drive its AI development efforts.[4]

Despite years of global investment in the development of these technologies from the U.S., China has the clear lead in certain areas of AI, such as computer vision. This was evident in a 2022 global aerial imagery detection contest when teams from China placed first, second, third and fifth .[5] The development of this technology has also extended to facial recognition technologies that are much more prevalent in China today than the U.S. While this may not present an obvious problem, it is concerning

[1] See, https://plato.stanford.edu/entries/turing-test/
[2] See, https://www.simplilearn.com/how-netflix-uses-ai-data-science-and-ml-article#:~:text=How%20does%20the%20Netflix%20algorithm,that%20the%20member%20has%20consumed.
[3] See, https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117
[4] See, https://2017-2021.state.gov/military-civil-fusion/
[5] See, https://paperswithcode.com/sota/object-detection-on-coco

because China is using its facial recognition technology to suppress the Uighurs and surveil its population.[6]

Since 2020, China has launched 79 LLMs[7], launched tens of national AI labs[8] and has been heavily investing in both the compute power necessary to power the AI[9] and the engineering talent to develop it. Additionally, this year alone, the Chinese government's investment into AI is $14.75 billion,[10] which stands in stark contrast to the President's FY24 budget proposal that calls for $5.5 billion in federal AI investment.[11] President Xi has made AI leadership a key tenet of his China 2025 plan,[12] highlighting it as a "historic leapfrog development opportunity,"[13] and China's state-sponsored AI development has been referred to as China's "Apollo Project."[14]

Currently, the best LLMs are all developed by some of the leading US-based engineers, and the data that they are trained on reflects our democratic ideals. It is imperative that the United States maintains this momentum if we want the most transformative technology of this era to reflect our leadership.

**GLOBAL AI GOVERNANCE PROPOSALS ARE ALREADY TAKING SHAPE**

To lead the world in AI adoption, we must also lead the world in the development of an AI governance framework that enables innovation while putting in place the proper

---

[6] See, https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-china s-surveillance-sta

[7] See, https://www.reuters.com/technology/chinese-organisations-launched-79-ai-large-language-models-since-2020-report-2023-05-30/

[8] See, https://thebambooworks.com/china-goes-it-alone-in-ai-2-0-drawing-on-local-funds-and-trio-of-industry-veterans/

[9] See, ft.com/content/47f7aefc-3ec0-4f66-80a1-24dcc551a845

[10] See, https://news.cgtn.com/news/2023-04-10/China-s-AI-market-spending-to-cover-10-of-world-total-in-2023-report-1iSPv1hUlWM/index.html#:~:text=Spending%20in%20China's%20artificial%20intelligence,International%20Data%20Corporation%20(IDC).

[11] See, https://www.pillsburylaw.com/en/news-and-insights/ai-biden-fy2024-budget.html

[12] See, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-calls-for-healthy-development-of-ai-translation/

[13] See, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

[14] See, https://thediplomat.com/2023/03/the-future-of-state-sponsored-ai-research-in-china/

guardrails. The U.S. has always led the world in the adoption of new technologies and crafting the right governance approach for them, although we have not necessarily been the first to implement regulations. AI will be no different.

Globally, there are no shortage of proposals being generated and passed. The European Union recently passed the EU AI Act.[15] Additionally, the United Kingdom[16] detailed a vision for AI regulation and China issued its own guidelines. There have been announcements out of the UN,[17] G20,[18] and more.

These frameworks all boil down to a few key questions, and the most important question is, "How do we know that AI is safe to deploy?"

To best answer this question, we must think about it throughout the entire AI development cycle. AI fundamentally comes down to compute power, a foundational model, and data. In the case of safe deployment of AI, I will focus on the foundational model and data because a model's performance is only as good as the data it is trained on. Scale has worked on nearly every generative AI advancement and LLM released. We have also pioneered many of industry's best practices today around data fine-tuning, red teaming, and test and evaluation.

**MODEL REFINEMENT & TESTING ARE CRITICAL FOR SAFE AI**

Our unique vantage point, working with all major companies in the space, has enabled us to understand how to make AI safe. Scale firmly believes that the best way to do this is through active and constant data fine-tuning, red teaming to expose unintended vulnerabilities, and then applying a risk-based approach to test and evaluation to ensure that the AI is safe to deploy.

AI safety begins with foundational training data that is then fine-tuned for specific use cases through a process known as Reinforcement Learning with Human Feedback (RLHF). In practice, the more RLHF completed on a model, the better performing that model will be as there is a direct tie between model performance and RLHF.

[15] See, https://artificialintelligenceact.eu/the-act/
[16] See, https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper
[17] See, https://press.un.org/en/2023/sgsm21880.doc.htm
[18] See, https://cointelegraph.com/news/g20-ai-use-and-development-india

After fine-tuning the data, it needs to undergo testing to uncover vulnerabilities through red teaming, followed by testing and evaluation procedures. These methods rely on industry best practices and consensus-based standards, offering the most reliable means to guarantee the safe deployment of AI for its intended purpose. It is crucial to adopt a risk-based approach that aligns the level of risk with an appropriately rigorous test and evaluation process.

This approach would ensure that higher risk activities, such as using an LLM for cancer research, undergo a more stringent evaluation process than a lower risk activity, like using LLMs for writing routine summaries. While all AI should go through this process, it is clear that certain use cases will require a higher bar.

Evaluation methods, including red teaming and benchmark tests, can incorporate the items that are critical to protect like copyrighted material, intellectual property (IP), and other sensitive topics. While industry still has work to do, this work is well underway.

Recently, Scale published our vision for test and evaluation[19] and will soon publish our technical methodology for our approach that builds on our work with OpenAI and the DoD's CDAO. This framework calls for a combination of machine and human testing, relying on red teaming, evaluation against leading frontier models and benchmark datasets, and human expert review. Once this methodology is released, we intend to work across industry to drive towards a consensus approach that will eventually turn into an industry standard for test and evaluation.

Industry standards are key for the safe deployment of AI and these standards currently are in the early stages of development. Once in place, this will give governments certainty that test and evaluation will be the right approach to ensure AI is safe to deploy. While standards already exist for items like cybersecurity, it is vital that we perform the proper policy gap analysis to best understand where new standards may be necessary for AI and ultimately work to fill the gaps.

For these reasons, the Biden-Harris Administration has recognized the value of red teaming and test and evaluation, both in the voluntary commitments that 15 leading

[19] See, https://scale.com/guides/test-and-evaluation-vision

companies, including Scale,[20] have agreed to and through their support for the DEF CON31 AI Village Red Team event in August 2023.[21] The voluntary commitments specifically call for, amongst other topics, internal and external red teaming and testing to ensure that AI adheres to the AI Bill of Rights blueprint and other responsible AI principles such as the DoD ethical AI principles.[22] Additionally, the recent DEF CON event saw over 2,200 participants red team eight leading LLMs on a test and evaluation platform built by Scale.[23] This event demonstrated the critical role that test and evaluation plays in both model development and ensuring AI is safe to deploy.

**ENSURING U.S. LEADERSHIP THROUGH THE RIGHT REGULATORY FRAMEWORK**

Beyond putting in place the right mechanisms to ensure the development of safe and responsible AI, it is clear that Congress must play a role to help enact the right governance structure. AI stands out for its ubiquity in people's everyday lives, ranging from machine learning algorithms to LLMs. The use cases for it and its centrality to our day-to-day lives will only continue to grow. Due to the importance of this, Scale fully supports Congress' approach to understanding the complexities of AI before working to legislate.

As mentioned above, we have already seen governments start to develop frameworks that will enable safe, secure, and trustworthy AI. These proposals all have their pros and cons, and are important to understand. However, putting in place an effective governance structure does not mean being first, but it does mean being right.

In the United States, we have also seen actions that are helping to establish the foundation for the right governance structure for AI. The 2019 AI executive order was

---

[20] See, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

[21] See,https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/

[22] See, https://www.defense.gov/News/News-Stories/Article/Article/3429864/dod-committed-to-ethical-use-of-artificial-intelligence/

[23] https://www.airedteam.org/news/more-than-2-200-participants-exchange-more-than-165-000-messages-with-leading-artificial-intelligence-large-language-models-during-the-generative-red-team-challenge

the first key step to help get our federal agencies ready to adopt AI.[24] More recently, the release of the NIST AI Risk Management Framework, blueprint for AI Bill of Rights, and the Biden-Harris voluntary commitments are essential precursors to any comprehensive legislative package. Additionally, the forthcoming executive order and updates to the procurement guidance will continue to move AI forward for the federal government.[25]

Much like other forms of emerging technologies, it is also important to first understand any deficiencies within the existing laws. Once these gaps are identified, we can take appropriate measures to address them through rulemaking or new legislation. For this reason, Scale supports regulating AI through the existing regulatory agencies, with a centralized coordinating body to focus on cross-cutting topics like research and development priorities.

A notable example of this process occurred with the emergence of the Internet and then video streaming, which initially posed challenges to the protection of copyrights and license agreements for text, music, and video content. After identifying the gaps in existing protections, industry and the government collaborated to develop solutions that are now considered the standard operating practices.

While it might feel urgent to act swiftly to keep up with global developments and maintain the United States' strategic advantage against China, one of the most important things we can do now is to establish the most effective regulatory framework that will ultimately be the approach adopted by the rest of the world.

**CONCLUSION**

Thank you again for the opportunity to be here today to discuss this critically important topic. All of my life, I have believed that the United States can and must demonstrate global leadership. I firmly believe that the U.S. must continue that leadership with the

---

[24] See, https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

[25] See, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

adoption of AI so America and the free world can reap the national security and economic benefits that will accompany it.

I look forward to your questions.