CENTER FOR
DEMOCRACY
& TECHNOLOGY

Statement of Alexandra Reeve Givens
President & CEO, Center for Democracy & Technology

U.S. Senate AI Insight Forum: Innovation
October 24, 2023

Senators, thank you for inviting me today. I am the President & CEO of the Center for Democracy & Technology (CDT), a 28-year old nonprofit, nonpartisan organization that works to protect users' civil rights, civil liberties and democratic values in the digital age.

CDT fights for policies and practices that protect users' interests — in areas ranging from commercial data practices, to the online information environment, to government surveillance, to the use of technology in schools and in government programs. AI is already transforming each of these areas, with the potential to profoundly affect society.

I'm particularly grateful to speak during the Insight Forum focused on innovation. Too often, public concerns about the risks of AI are dismissed as "anti-innovation." My message today is simple: **Congress must reject the idea that addressing AI harms is somehow counter to innovation. America can lead the world by creating technology that *works*, is safe, and protects people's rights.**

A brief survey of the current AI landscape demonstrates this point. Across all sectors of the economy, businesses, organizations and individual users are deciding whether to adopt AI tools and systems – and they need confidence in how those systems are designed, tested, and deployed. Today, a small business owner deciding whether to use an automated AI hiring tool has no meaningful rubric or visibility to assess whether the tool may discriminate against some job candidates, exposing the business to legal and reputational risk as well as missed talent. A person deciding whether to use a generative AI tool has to rely on companies' hard-to-judge assertions about accuracy, bias mitigation, data privacy and security. Given the fast pace of technological advancement and asymmetries in power and information between AI companies and customers, legislation will play an essential role in creating baseline standards to earn people's trust.

Importantly, there has been helpful convergence in the past few years around the key elements of trustworthy AI. The National Institute of Standards and Technology's AI Risk Management Framework and the White House's Blueprint for an AI Bill of Rights each spell out basic expectations for trustworthy AI systems:

- systems must be safe and effective (in NIST's words, assessed for validity and reliability, security and resiliency);

- systems and tools must not discriminate or have harmful bias;
- systems must protect people's privacy and data security;
- systems must come with notice and explanation, accountability & transparency; and
- where appropriate, systems should be subject to human alternatives, consideration and fallback.[1]

Requiring AI systems to embody these basic values will not curb innovation. To the contrary, these basic values are the way to ensure American technology works, is safe, and protects people's rights.

As Congress begins its legislative process, it should use these elements of trustworthy AI as a north star for responsible innovation – and combine regulation with research investments to help companies of all sizes achieve them.

There are several steps Congress can take towards this goal.

First, **Congress should develop requirements for auditing/impact assessments** to ensure that companies designing and deploying AI tools analyze how they work, account for potential risks, and document the steps taken to mitigate those risks. This type of risk management process should be part of any normal business operation, but Congress can drive this behavior and ensure a level playing field by codifying AI risk management into law. Critically, Congress must do this in a way that allows downstream deployers, end users, and subjects of an AI system to gain appropriate understanding about the system's risks and limitations – and for the public and regulators to gain necessary insights. AI assessments must take place not just when an AI system is first developed, but on an ongoing basis in the context where it is deployed. Congress will also need to ensure that any auditing/assessment legislation is actually effective: that it doesn't allow companies to simply self-certify compliance with a vague set of standards that do not, in fact, address potential risks and harms. We understand important work is happening among Members on this issue, and we commend your focus on this essential component of trustworthy innovation.

Second, **Congress should mandate baseline protections for civil rights, data privacy and data security.** An immediate step Congress could take to address certain AI harms is to pass long overdue comprehensive privacy legislation. Core privacy principles such as data minimization (including heightened protections for sensitive information), civil rights, user rights, and algorithmic transparency all serve to reduce harms related to AI training and outputs.

[1] *See* National Institute for Standards & Technology, AI Risk Management Framework (2023), https://www.nist.gov/itl/ai-risk-management-framework; White House Office of Science & Technology Policy, Blueprint for an AI Bill of Rights (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

But short of passing comprehensive privacy legislation, any AI legislative package should – indeed, must – contain core provisions to address those AI-related harms. In particular, legislation should prohibit discrimination by AI systems and ensure testing, transparency, and explainability to help people identify how a system may discriminate against them, and how to vindicate their rights. Legislation should establish baseline privacy protections for AI systems, especially regarding sensitive data, and ensure data security.

Third, beyond these cross-cutting protections, **Congressional committees should develop sector-/use-case specific legislation to address various high risk uses of AI** – such as, for instance, legislation to address the biosecurity and national security risks of emergent frontier models, or to address consumer fraud and extortion schemes that use deepfake audio and video. To give one example, the Senate Banking Committee is rightly examining the impact of AI in our financial systems: here, as in other sectors, Congress can examine the effectiveness of existing laws, consider tailored legislative updates, and (through oversight and appropriations) ensure that regulatory agencies are providing the industry guidance and regulatory protections that this moment requires.

Fourth, **Congress should ensure the United States is a world leader in the government's responsible use of AI.** Much ink has been spilled on how America's AI policy must compete with China. There's no clearer way for the U.S. to distinguish itself from China than by showing how a *democracy* uses AI in a manner that respects its people's rights. Congress has already passed several laws to improve the federal government's AI readiness and directed the Office of Management & Budget to issue binding guidance on the federal government's use of AI. As the Biden Administration pursues this work, Congress can appropriate funds and create new mechanisms to ensure the U.S. government is truly leading the world by example, with meaningful standards, transparency, and public accountability, including for systems that are procured from the private sector.

Finally, **Congress should ensure that federal AI research and government-supported Standards processes advance methods for evaluating, testing, and mitigating AI harms.** As Congress invests in federal research, it must dedicate funding to help answer the hard challenges involved in measuring and mitigating bias, achieving explainability, ensuring effective transparency, and other key elements of trustworthy AI. The National AI Advisory Committee, a Congressionally-mandated body of experts from industry, academia and civil society, has emphasized this need, urging financial support "for a strong research base and community of experts; for meaningful, usable, and extensible measures of social considerations for AI development and implementation; for frameworks to support future standards; and for standards and best practices which support future policy."[2]

Nowhere is innovation more urgently needed than in methods for evaluating and testing AI systems and their impacts, and successfully mitigating risks to people's rights, safety, and broader environmental harms. Again, with thoughtful action and investment by Congress, the United States will be positioned to lead in AI standards efforts and methodological advances taking shape around the world.

–

Last week, CDT and a coalition of almost 90 public interest organizations wrote a letter to Congress urging you to prioritize the varied ways in which AI is already impacting our economy and society.[3] We wrote, "For the United States to be a true global leader in AI, it must lead in responsible, rights-respecting innovation that directly addresses these myriad harms." Only with attention to these issues can we be confident that the U.S. is leading in *responsible* innovation, protecting its people, and helping businesses and government agencies know when they can trust and responsibly use emerging AI tools.

[2] National AI Advisory Committee, Year One Report at 37 (May 2023), available at https://www.ai.gov/wp-content/uploads/2023/05/NAIAC-Report-Year1.pdf.

[3] Letter to Congressional leaders from 87 public interest organizations regarding AI Insight Forums, hearings and legislative efforts (Oct. 17, 2023), available at https://cdt.org/wp-content/uploads/2023/10/10-17-23-Public-Interest-AI-Letter-to-Congress.pdf.