Submitted Statement of

Brandon Pugh
Policy Director and Resident Senior Fellow,
Cybersecurity and Emerging Threats
R Street Institute

Before the

Bipartisan Task Force on Artificial Intelligence
United States House of Representatives

Meeting on

Privacy, Transparency, and Identity

June 28, 2024

Chairman Obernolte, Co-Chair Lieu, and members of the Task Force:

Thank you for inviting me to participate in today's task force meeting. I am fortunate to lead the cybersecurity and emerging threats team for the R Street Institute, a nonprofit, nonpartisan, public policy research organization aiming to promote free markets and limited, effective government.

I'd like to begin by thanking the task force for its exploration of artificial intelligence, especially from a framing that we must ensure America leads the world in AI innovation while recognizing that some guardrails might be necessary.

Data privacy is a great example for this as AI has the potential to both strengthen and foster privacy. In many ways, it already has. But AI also requires guardrails to ensure consumer privacy is maintained and that data is adequately secured. I have two main recommendations for the taskforce to pursue: first, acting on a comprehensive federal data privacy and security law that remains focused on privacy, but considers the implications on AI, and second, encouraging efforts to safeguard our data and recognizing that AI is a key part of that.

Speaking to my first recommendation, the need for a federal comprehensive data privacy law is more timely now than ever given the increased usage of AI. As we know, AI is about data at its core. Therefore, it is critical to have a federal approach that increases transparency, protects consumers' rights, and secures data. For any version to pass, compromise will be important.

I believe a federal comprehensive privacy law should balance the needs of consumers, innovation, and security. There are a number of ways this must be done, but I can flag five that I am happy to expand on later or identify others. Any law must:

1. *Focus on privacy*, rather than venturing into broader considerations like specific AI measures. I believe privacy is applicable across all forms of technology, so it is ideal to have a framework that can be applied broadly with more specific measures considered separately;
2. *Not unduly limit innovation*. This includes ensuring a law is applicable to data uses that we might not be considering or even know of. It should also look to incentivize further innovation, like the use of privacy enhancing technologies (PETs);
3. *Protect consumers' rights and ensure transparency* into how their data is collected, used, and transferred. After all, most Americans do not enjoy this now absent those in less than twenty states and most blindly accept privacy notices without reading or understanding them;
4. *Ensure compliance,* and more importantly, the *ability* to comply, by all types and sizes of businesses. This is particularly important for AI as many companies doing amazing research and deployment are small and resources shouldn't needlessly be used to comply with a new law; and finally, any law must
5. *Preempt* state and local privacy and data security laws so that there is one standard, rather than the patchwork we see today, which leads to gaps in protections by Americans and costs on industry that could be better allocated elsewhere.

As to my second recommendation, we should encourage efforts to safeguard our data and leverage AI to do so. We know bad actors, whether nation-states or criminal groups, will continue to try to steal and exploit our data, especially sensitive data. Given the amount of data utilized by AI at all stages, especially when it leverages either classified or sensitive data, we must ensure it is adequately protected.

I often hear of concerns around how AI might present cybersecurity risks. There are risks, but I am very encouraged by how AI has been leveraged in both data security and cybersecurity already. The R Street Institute convened an AI and Cyber working group that met over the course of about nine months with fifteen members from academia, civil society, industry, and Capitol Hill. In particular, we were thrilled to have representation from your office, Mr. Chairman.

Our findings convey that there are many current uses of AI for cyber defense; that future innovations underway should be encouraged and not unduly limited by AI regulation or legislation; and that while there are risks from a security front, they should be addressed proactively and in an even-handed manner.

Thankfully, when it comes to both data privacy and data security, we already have a firm foundation. Many agencies have expertise in this space, including with providing guidance like the National Institute of Standards and Technology’s cyber, privacy, and AI frameworks. In addition, some agencies have taken enforcement actions against bad actors, and many in industry have proactively embraced privacy and responsible AI measures. However, there is still much to consider as the technology landscape evolves and expands, which will require balanced solutions by all to ensure we continue as a leader in both AI and privacy.

Thank you again for holding this session. I look forward to answering your questions today. And of course, I am always happy to be a resource to you and your staff moving forward.