COMMITTEE ON
SCIENCE SPACE
AND TECHNOLOGY

Opening Statement of Investigations and Oversight Subcommittee Chairman Jay Obernolte

Joint Subcommittee on Investigations and Oversight and Research and Technology Hearing

Balancing Knowledge and Governance: Foundations for Effective Risk Management of Artificial Intelligence

October 18, 2023

Good afternoon. Welcome to what I am hopeful will be a very fruitful discussion on foundational questions Congress needs to answer to ensure that we strike a careful balance between protecting consumers and protecting innovation as we create a regulatory framework for artificial intelligence.

Earlier this summer the Science Committee held a hearing to explore how Congress can ensure that AI technology advances our national interest.

One of the unifying takeaways was that there remains a number of unsolved technical challenges which, if addressed, would advance innovation while making AI systems safer, more transparent, and easier to implement guardrails around.

Today’s hearing will build upon that theme by exploring how the Science Committee can support research, testing, and the deployment of methods and tools for managing AI risks. These tools and methods will be critical to the good governance of these systems as Congress examines how it should regulate AI.

I believe that fundamental research on AI is a necessary precondition for safer systems. While regulations can make undesirable actions unlawful, technological advances and coordination with other countries in monitoring who has access to the compute necessary to train frontier AI models and how it is being put to use will be critical tools in supporting and enforcing regulations.

One example is the use of confidential computing to make the theft of AI models more difficult. It is currently relatively straightforward to steal an AI model because the data needed to operate the model—known as the model weights—is stored in raw files. Stealing these files would allow criminals to use the model without spending the millions of dollars on compute and data necessary to train the model. Stricter cybersecurity laws can only go so far to prevent this from occurring. However, recent research into confidential computing could potentially enable the model to be operated without allowing access to the model weights, rendering cyber-theft impossible and addressing the root cause of the problem.

Another challenge that advances in research can help resolve is identifying whether AI has been used to generate content. It is clear that instances of identity fraud, plagiarism, and a host of other issues will become more common as the power of AI tools increases. Watermarking is a technique whereby digital content is encrypted with unique, often hidden, identifiers that provide information about its origin. Watermarking has the potential to identify the origin of any content regardless of how it was created or digitally altered. Although current discussions of watermarking center on a desire that AI-generated content be watermarked, watermarking can also be used to prove the provenance of authentic content. In fact, it is entirely possible that in the future, people may automatically assume that all content is AI-generated unless its watermark proves its authenticity.

Solving this technical problem would enable a new set of good governance tools concerning generative AI that were previously infeasible.

These examples illustrate the fact that research and policy are not mutually exclusive, but in fact mutually dependent. Research advances unlock previously unpractical approaches to regulation, and smart policy accelerates research.

I believe that we must also standardize technical definitions for methodologies, risks, and technological concepts across the government. The NIST AI Risk Management Framework lays out a foundation that other agencies can build upon. As these agencies consider passing rules or using procurement authorities to incentivize good behavior, they should ensure a consistent methodology for assessing risk levels and tailor their policies accordingly.

Another technical area in which Congress has a crucial role to play is promoting and establishing best practices. This includes everything from technical standards to evaluation benchmarks for testing the trustworthiness and risks of AI systems.

Let us not forget that while Congress should certainly not rush to overregulate, we should also not be complacent. The U.S. must avoid falling behind other major world powers who are finalizing their AI standards and regulations.

Without proactive American leadership, supremacy in AI could be seized by the EU or China, both of which are taking far more draconian approaches to AI regulation.

Because the U.S. currently leads the rest of the world in AI research and development, it makes no sense for us to stand by while American companies are forced to either make educated guesses or play by others' rules.

We must also ensure that our academic institutions continue to play an active role in research and development of AI, and that the transparent system of publication and peer review that has enabled its success thus far is not replaced with an opaque system where cutting-edge research is only performed by corporations. This is why I believe is it critically important that we establish a National Artificial Intelligence Research Resource (NAIRR) as a shared national research infrastructure to ensure researchers have access to the tools needed to test, develop, and create new AI-backed technologies. This idea was proposed earlier this Congress when I joined my fellow AI Caucus Chairs in introducing H.R. 5077, the Creating Resources for Every American To Experiment with Artificial Intelligence Act (CREATE AI Act). Establishing a shared computing and data infrastructure resource, such as that detailed in the Act, would democratize access to AI by providing researchers and students across scientific fields and disciplines with access to compute resources and high-quality data, along with appropriate educational tools and user support.

I want to thank all our witnesses for taking the time to join us today for this important discussion.

I look forward to hearing your recommendations for how this committee can strengthen our nation’s leadership in artificial intelligence and set clear rules for the safe, responsible, and human-centered development of this exciting new technology.