Testimony of Matthew Reisman

Centre for Information Policy Leadership

September 18, 2025

Thank you, Chairman Steil, Vice Chairman Emmer, Ranking Member Lynch, and members of the Subcommittee for the opportunity to be with you today. I am Matthew Reisman, Director of Privacy and Data Policy at the Centre for Information Policy Leadership, or CIPL, a data and privacy policy think tank within the Hunton law firm whose mission is to advance best practices for the responsible and beneficial use of data in technology and society. CIPL facilitates constructive engagement between business leaders, data governance experts, regulators, and policymakers around the world.

AI plays a critical role in the financial services industry, as this Committee documented well in the staff report of its bipartisan Working Group on Artificial Intelligence. For years, machine learning has strengthened financial services institutions' ability to combat fraud, provide richer and more tailored services to existing customers, and extend services to new ones. More recently, generative AI has boosted productivity across functions, from software development to customer service. And we are now in the early days of agentic AI, which shows promise for enhancing the experiences of businesses and customers alike. Potential applications in the sector are extensive, from streamlining Know Your Customer processes, to back-office operations like payroll and invoicing, to online banking, to shopping powered by agentic commerce.

AI's use in financial services also carries risks – to consumers, the institutions using the technology, and the financial system. The bipartisan staff report documents these risks well. Like AI solutions before it, agentic AI may accentuate some risks while at the same time enhancing our risk management capabilities, in areas such as privacy and cybersecurity.

To responsibly secure the advantages of AI within the financial system, we have three recommendations:

First, with respect to regulation, pursue a risk-based approach that focuses on the outcomes to be achieved. Avoid overly prescriptive measures. Build upon existing foundations, including regulations, guidance, and standards already in place. When necessary, clarify or adapt their application to emerging technologies. Consider risks and benefits in equal measure. Incentivize organizations to adopt accountable practices. Build trust through meaningful transparency. CIPL has long underscored that these concepts of organizational accountability are central to smart governance of data and technology.

Second, enable the responsible use of data for model training and development. To function effectively, safely, and fairly, models must be trained and tested using rich datasets. Regulators should apply data protection principles in ways that ensure the

quality of AI systems, while upholding the privacy of individuals. Privacy-enhancing technologies, or PETs, can reduce risks associated with the use of personal data. Examples include synthetic data—artificial data that mimics the values of real-world data—and differential privacy, where random "noise" is added to datasets to prevent identification of any individual's data. Policymakers should encourage continued research on and use of PETs.

Third, engage in cooperative dialogue among regulators, technologists, and industry. As AI continues to evolve rapidly, stakeholders must learn from each other to harness technology's benefits and mitigate risks. Fostering such exchanges is the heart of CIPL's mission, and regulatory sandboxes offer an invaluable avenue for them. Numerous jurisdictions around the world have established regulatory sandboxes for technology over the past decade, from the UK, to Singapore, to U.S. states like North Carolina and Delaware. We commend steps to promote sandboxes under America's AI Action Plan; the proposed bipartisan, bicameral Unleashing AI Innovation in Financial Services Act; and other proposed legislation.

CIPL has published numerous reports which explore these topics in greater detail. They can be accessed through our website (www.informationpolicycentre.com).