Statement of Stu Ingis, Chairman of Venable LLP,
at the Sixth U.S. Senate AI Insight Forum: AI, Privacy & Liability
Wednesday, November 8, 2023

Thank you, Majority Leader Schumer, Senators Rounds, Heinrich, and Young, and Distinguished Members of the Senate for organizing these AI Insight Forums and for inviting me to speak. It is an honor and a pleasure to join you today and be a part of the continued discussions on the appropriate governing principles for artificial intelligence (AI).

My name is Stu Ingis, and I am the chairman of Venable LLP. I have spent three decades building coalitions, working with policymakers and the business community developing industry standards and best practices for the responsible use of data. These efforts include technology and industry groups focused on privacy and technology, such as the Alliance for Trust in AI and Privacy For America. These organizations represent companies across a broad cross-section of the American economy, including companies and trade associations in the advertising, travel, hospitality, media, retail, manufacturing, financial services, and data services industries, as well as many others.

Artificial Intelligence Governance

The potential benefits of AI are clear and profound, and can foster improvements in every aspect of life: healthcare, logistics, security, consumer products, education, work, and much more. This sixth bipartisan AI Insight Forum, on privacy and liability, should focus on ways to support cross-sector use of AI in ways that protect privacy and data while enabling AI use.

As a field, AI is moving quickly. While it has been used for decades, new tools are becoming available to the public, industry, and the government at an increasingly rapid pace. Stakeholders in AI development, deployment, and utilization should work together to shape policies that maximize the benefits of AI and prevent unintended and harmful consequences.

We, as a society, need to know that we can trust the AI underlying the products and technologies we use for business and as individual consumers. The Alliance for Trust in AI is doing just that – bringing together companies who are using AI with responsible and thoughtful governance to discuss best practices and principles across industries to establish and maintain that trust.

While the implementation and operationalization of AI tools will necessarily vary across industries, there is room for a shared understanding of how to use and develop AI. The Alliance for Trust in AI is developing in partnership with members across industries principles and codes of practice that allow developers and implementers of AI systems to demonstrate responsibility and accountability. This allows creation of an overarching set of principles and sector-specific guidance in the form of codes of practice to interpret those principles. In following these codes, stakeholders using AI can build trust by shifting their focus towards responsible and accountable use, rather than an abstract set of ethics.

To facilitate a future where AI is trusted and accountable, we should lean into accountability, self-regulation, and governance, working in partnership across industry and government as we work to manage risk and ensure that everyone can realize the opportunity that all kinds of AI provide. Accountability is an important part of a framework for responsible development and use of AI, but matters of liability must be aligned appropriately so as not to have a chilling effect on AI and innovation.

Privacy and Artificial Intelligence

Data is vital to AI. Many kinds of technologies use AI, and in turn AI is used in many ways. One thing that all advanced AI has in common is data. AI is dependent on data. It is core to creating AI models, to machine learning, and - often - AI is used to sift through large amounts of data to create predictions, find anomalies, and detect threats. As a result, using data responsibly is key to ensuring that AI is trusted. Quality data is vital to quality training of AI models, which can then operate accurately, appropriately, and fairly.

When AI intersects with personal data or the lives of human beings, extra care should be taken. Privacy should be considered throughout AI model development and implementation to ensure appropriate data use. The confidentiality and sensitivity of input and output data should be considered, especially in contexts where AI-based determinations impact rights and eligibility for certain opportunities.

Data use in AI helps ensure bias mitigation, representation, more accurate results, and consumer protection. A commitment to accurate, representative, and comprehensive data is a part of effective AI governance. To ensure that AI systems are operating properly, developers must have accurate, representative, and comprehensive data about these interactions. Using representative training data when creating or improving AI systems is fundamental to ensuring they accurately represent the diversity of communities. If it is available, data can be used to evaluate whether the system is introducing unintended bias and allow for continual recalibration of AI systems to correct unwanted behaviors. Accurate and timely data about interactions and transactions allows systems to monitor for cybersecurity threats and fraud, protecting both the deployed AI system and its users.

AI developers, implementers, and users should be transparent about data used in AI. There are ways to help people understand the data that is used to train these systems and what they are intended to do. Best practices for explainability and transparency of AI systems are still being developed, but transparency for users is a core value for data privacy legislation and should be a core element of AI governance as well. Such clarity is key to building trust and making sure AI is used responsibly.

Sustainable privacy practices require sustainable privacy governance, which is a more appropriate way to ensure that data used responsibly than broad restrictions. Self-regulatory approaches have been used successfully across many dynamic industries and markets and ensure that there is a shared understanding of expectations and best practices with enforcement entities to ensure action. This also allows frameworks to be prompt, flexible, and responsive to the evolution of how companies and other organizations are using AI. Ensuring accountability

through risk management that reflects the industry and context in which AI is used is core to many of the recent frameworks supported by the Administration: the recent Executive Order, the G7's Hiroshima Process Principles and Code of Conduct, and the Bletchley Park Principles. Even the European Union's AI Act takes this approach. This global focus on risk management and accountability has the potential to effectively guide the development and use of AI, especially if we ensure that an American framework takes a similar approach.

Congress should pass a federal, preemptive privacy law. All of this is not to say that Congress should not act. A comprehensive, preemptive federal consumer data privacy would make personal data less vulnerable to breach or misuse and set forth clear, enforceable, and nationwide consumer privacy protections for the first time. Taking a co-regulatory approach can support industry use of AI at the same time as it protects data. Providing clear rules for the data that AI depends on, balancing the need for data to power these systems with strong privacy protections, will serve to increase the opportunity for development and use of AI for all sectors of the economy.

Conclusion

Thank you for inviting me today. As we work together to align our societal goals with the technology we build, and the governance we impose, I look forward to working with you and across industry. We welcome partnership as you work to facilitate responsible use of AI to support the American people and the American economy, and I look forward to your questions today and in the future.