ITI Promoting Innovation Worldwide

Written Testimony of

Rob Strayer

Executive Vice President of Policy

Information Technology Industry Council (ITI)

Before the

United States Senate Committee on

Commerce, Science, & Technology

Subcommittee on Consumer Protection, Product Safety and Data Security

Hearing on

The Need for Transparency in Artificial Intelligence

September 12, 2023

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Chairman Hickenlooper, Ranking Member Blackburn, and Distinguished Members of the Committee and Subcommittee, thank you for the opportunity to testify today.

My name is Rob Strayer, and I'm the Executive Vice President of Policy at the Information Technology Industry Council (ITI). I lead ITI's global policy team, driving ITI's strategy and advocacy efforts to shape technology policy around the globe and enable secure innovation, competition, and economic growth, while supporting governments' efforts to achieve their public policy objectives. ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry. We represent leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, Internet companies, and other organizations using data and technology to evolve their businesses. Our members stand at the forefront in developing and deploying consumer-facing, business-to-business, and government-focused AI solutions.

We are encouraged by the bipartisan efforts in Congress to address the challenges and opportunities from AI. This subcommittee's jurisdiction over issues ranging from data privacy and consumer protection to standards gives you an important role to play in AI policy discussions. To that end, ITI was pleased to provide information to Chairman Hickenlooper and Ranking Member Blackburn's inquiry earlier this year about how ITI members are operationalizing NIST's AI Risk Management Framework (AI RMF) to build and foster public trust.[1] Congress and the Administration should work together to ensure any legislation or regulatory proposals encourage future innovation and investment in the United States, protect consumers and businesses, mitigate foreseeable risks, and do not complicate or duplicate existing standards, laws, and sector-specific regulatory regimes. ITI looks forward to being a partner in those efforts.

I. Transformational Impact of AI

The development and adoption of AI technologies will be transformational across a variety of critical sectors, including health care, telecommunications, aerospace, manufacturing, transportation, and other sectors under the Committee's jurisdiction. It will help companies be more effective and efficient, particularly at addressing business operations challenges, research and development, and software engineering. In fact, an Accenture survey of 1,500 executives across all sectors found that 84 percent believed AI is critical to meeting their growth objectives and 73 percent said they risk going out of business if they cannot scale AI.[2]

[1] ITI's June 2023 response to Chairman Hickenlooper and Ranking Member Blackburn's April 2023 letter (June 1, 2023) *available at*: https://www.itic.org/documents/artificial-intelligence/ITIJune2023ResponsetoSens.HickenlooperandBlackburnAIRMFLetter.pdf

[2] *See* Accenture AI investment study (November 14, 2019), *available at* https://www.accenture.com/us-en/insights/artificial-intelligence/ai-investments

As a testament to AI's revolutionary impact, credible estimates of the **total global economic benefits of AI in the years ahead, which now includes the impact of generative AI, range from $14 trillion to $25 trillion.**[3]

Today, the United States is leading AI development, deployment, and innovation. The United States employs the best and the brightest AI researchers and experts working to advance American leadership in AI innovation. Other nations have recognized the United States as the center for AI excellence and are working harder than ever to develop the next major technological developments in AI and to deploy AI in new use cases in their countries.

Policymaking and regulation involving AI needs to be understood in the global context of technology competition. **The United States has the potential to build on its lead as AI transforms all sectors of the economy, generates trillions of dollars in economic growth, and benefits U.S. companies and citizens for decades into the future. Overly broad and prescriptive regulation, however, could undermine that leadership position and cede it to U.S. competitors, including authoritarian nations.**

AI will play an essential role in future national security applications for the military and intelligence communities and in the cybersecurity defense of critical infrastructure. It is not an exaggeration to say that U.S. national security depends on continued U.S. technological leadership in AI. It is more important than ever that the United States considers how any new policy affecting AI will help it maintain its technological leadership in AI.

Below are some of the use cases that AI will empower:

- **Cybersecurity**
    - *Threat Mitigation*: AI and machine learning can be leveraged to improve cybersecurity. Indeed, defensive cybersecurity technology must embrace machine learning and AI as part of the ongoing battle between attackers and defenders. The threat landscape constantly evolves, with cyberattacks that are complex, automated and constantly changing. Attackers continually improve their sophisticated and highly automated methods, moving throughout networks to evade detection. The cybersecurity industry is innovating in response: making breakthroughs in machine learning and AI to detect and block the most sophisticated malware, network intrusions, phishing attempts, and many more threats.[4] AI is the best tool defenders have to identify and prevent zero-day attacks and malware-free attacks because AI can defeat novel threats based on behavior cues

[3] *See* McKinsey and Company *The Economic Potential of Generative AI: The Next Productivity Frontier* (June 2023), *available at* https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivity-frontier-vf.pdf?shouldIndex=false

[4] Testimony of Rob Strayer, Hearing on Securing the Future: Harnessing the Potential of Emerging Technologies while Mitigating Security Risks, Before the U.S. House Homeland Security Committee (June 22, 2022) *available at* https://www.itic.org/documents/cybersecurity/20220622ITIHouseHomelandCmteTestimonyonEmergingTechandCyber.pdf

rather than known signatures. Leveraging these technologies is essential to meeting constantly evolving threats.

- **Manufacturing**
  - *Predictive Maintenance*: AI can analyze real-time sensor data from manufacturing equipment to predict maintenance needs accurately. By identifying potential equipment failures in advance, manufacturers can schedule maintenance proactively, minimizing unplanned downtime and reducing costs.
  - *Supply Chain Management*: AI can optimize supply chain operations by analyzing data from multiple sources, including demand forecasts, inventory levels, and logistical constraints. AI algorithms can optimize inventory management, improve demand forecasting accuracy, and enable efficient routing and scheduling of shipments.

- **Health Care**
  - *Medical Imaging Analysis*: AI can analyze medical images such as X-rays, CT scans, and MRIs, helping doctors detect and diagnose diseases more accurately and efficiently. AI can assist in identifying anomalies, tumors, or other abnormalities, leading to earlier detection and treatment.
  - *Drug Discovery and Development*: AI accelerates the drug discovery process by analyzing massive datasets and identifying potential drug candidates. AI algorithms can predict the efficacy of drugs, design molecules, and optimize clinical trials, reducing the time and cost of bringing new drugs to market.

- **Telecommunications**
  - *Network Planning and Deployment*: AI can help analyze data to assist in planning the deployment of telecommunication networks. AI can help determine optimal tower locations, estimate coverage areas, and predict network capacity requirements, enabling providers to make informed decisions during network expansion.
  - *Network Security*: AI can monitor network traffic, detect anomalies, and identify potential cybersecurity threats. AI algorithms can analyze patterns, identify malicious activities, and take immediate action to protect the network and customer data from cyberattacks.

II. The United States needs to develop a pro-innovation policy framework that appropriately manages risk while maintaining U.S. technological leadership.

ITI's AI policy framework has four key pillars: 1) fostering innovation and investment, 2) facilitating public trust in and understanding of the technology, 3) ensuring security and privacy, and 4)

maintaining global engagement.[5] My testimony today primarily focuses on the first two, although a comprehensive framework should seek to address all the above policy pillars.

A. A pro-innovation policy framework should support innovation and investment.

While much of the conversation of late has focused on ways in which to foster accountability, **there needs to be at least equal attention given to fostering innovation and investment.** Continued investment in AI research and development, by both the government and private sector, is essential for the United States to maintain its leadership position. ITI applauds the funding and authorizations in the CHIPS and Science Act for federal efforts to enhance U.S. technological leadership in AI and other emerging technologies.

Regulatory policies that encumber the ability of researchers and developers in the United States will drive investments and research activities into other countries. Through open-source models and platforms, access to AI capabilities will be placed increasingly in the hands of a growing number of innovators of all sizes. This combined with decreasing costs for AI compute training resources, which are estimated to decrease 70 percent annually, will allow innovators to migrate away from jurisdictions with stifling regulations.

Most funding for AI research and development will come from the private sector. Smart technology investment-related tax policies and market incentives can encourage greater investments by the private sector that will produce AI innovations. ITI has detailed its views on these tech policies elsewhere.[6]

Government sponsored research in AI also has a role. Government investments in foundational science and AI-specific program research are important to fill gaps. Research by academia and the private sector into privacy enhancing technologies (PETs) and in measurement science to test, evaluate, validate, and verify (TEVV) model performance are critical to effectively implementing a risk management approach. **Innovations in measurement tools for AI will make risk management more concrete and objective and improve accountability and transparency.**

The government also has a role in incentivizing professional and technical apprenticeships, education and training programs in STEM fields, and promoting access to external and online reskilling programs. AI is not just a function of STEM or advanced technical training; the best way to ensure access to an AI workforce is to invest broadly across all relevant disciplines and teach flexible skills and problem solving from early childhood education.

[5] See ITI Global AI Policy Principles, *available at* https://www.itic.org/documents/artificial-intelligence/ITI_GlobalAIPrinciples_032321_v3.pdf

[6] See, e.g., https://www.itic.org/news-events/techwonk-blog/congress-must-act-to-support-us-research-and-development

B. A pro-innovation policy framework should be risk-based, evaluate the existing regulatory landscape, and clearly delineate risk areas that are not adequately addressed.

In seeking to support innovation, it is important that we understand the risks that we are seeking to address with a regulatory framework. AI will continue to evolve, and we need to address risks as they develop, while not suppressing the advancement of AI.

Risks need to be identified and mitigated in the context of the specific AI use. This will help policymakers determine use cases or applications that are of particular concern, avoiding overly prescriptive approaches that may serve to stifle innovation. Beyond that, context is key. Not all AI applications negatively impact humans, and thus, they cannot inflict harm that would warrant regulation.

With those risks identified, the next step is to consider the role for existing statutory and regulatory authorities to address discrete risk. We don't want layers of regulation that conflict with one another, create undue burdens on innovators, and slow advancement.

Therefore, it is imperative that the government review the existing regulatory landscape to assess where there might be gaps. **There are existing laws and regulatory frameworks that can address AI-related risks, so it is critical to understand how those laws apply, and where they may not be fit-for-purpose, prior to creating new legislation or regulatory frameworks pertaining to AI.**

As an initial step, policymakers should evaluate how NIST's AI RMF is being adopted and how it can be used to manage risk. The AI RMF provides companies with a comprehensive way to think about risk management practices, which is fundamental to fostering long-term public trust. It captures many of the outcomes and best practices that companies are already undertaking, such as framing and prioritizing risks and addressing AI trustworthiness characteristics (e.g., reliability, safety, explainability, privacy, fairness, accountability, and transparency). ITI and its member companies were active in the development of this Framework and are actively adopting it. We appreciate that NIST has also launched the AI RMF Playbook as a complement to the AI RMF. Indeed, this tool is instrumental to ensuring that the Framework is actionable and implementable, particularly for organizations that may be less familiar with the scope of guidelines and best practices that are available to them. In recent comments to the Office of Science and Technology Policy, we encouraged the Administration to explore how the AI RMF might be integrated into federal contracts and encouraged the government to leverage the AI RMF in crafting forthcoming guidance. [7]

Conducting a robust gap analysis of existing legal authorities relevant to AI's potential harms is critical because there are many laws and regulations that can address the diversity of impacts implicated by the technology. Some of these relevant bodies of law and regulation, coupled with relevant potential AI-related harms, include: intellectual property law, especially the Copyright Act of 1976, to address

[7] *See* ITI's July 2023 response to OSTP RFI, re: ITI Response to Office of Science and Technology Policy Request for Information on National Priorities for Artificial Intelligence, *available at* https://www.itic.org/documents/artificial-intelligence/ITIResponsetoOSTPRFIonNationalAIPrioritiesFINAL%5B25%5D.pdf

issues related to the use of copyrighted material in training data and questions regarding the IP rights in AI generated content; the Federal Trade Commission Act to address unfair, deceptive or abusive practices related to AI-enabled misrepresentations or harmful content; product liability common law to address potential safety issues related to products containing AI technology that may cause physical injury; First Amendment jurisprudence and Section 230 of the Communications Decency Act to address issues related to AI-generated content and freedom of expression interests; Title VII of the Civil Rights Act of 1964 and related laws to address issues related to bias, discrimination, or other civil rights harms; and relevant federal sector-specific privacy provisions, such as in the Health Insurance Portability and Accountability Act, to address potential privacy harms related to AI that include the accuracy of data.

In our view, it makes sense to proceed with creating new legislation only if there is a specific harm or risk where existing legal frameworks are either determined to be insufficient or do not exist.

Regarding privacy protections, as noted above, privacy laws do exist that can address some AI-related privacy harms. Yet, there is also an undeniable regulatory gap given the absence of federal privacy legislation. ITI testified before the House Energy and Commerce Committee in 2022 in favor of preemptive federal comprehensive privacy legislation, which we consider critical to protecting consumers from data related harms and a necessary complement to any potential AI legislation or regulation.[8] However, ITI urges the Committee not to conflate potential AI legislative provisions with comprehensive privacy legislation. For example, in ITI's testimony on the American Data Privacy and Protection Act, we expressed concerns that the bill conflated the two issues by prematurely including prescriptive requirements to conduct algorithmic design evaluations and impact assessments, and that the scope of those requirements, which would have potentially covered all algorithms, were overbroad and would have swept in a vast array of technologies well beyond AI.

C. A pro-innovation policy framework should aim to foster public trust in the technology.

The guiding goal of an AI policy or regulatory framework should be fostering public trust in AI technology. Fostering trust in AI systems[9] requires AI model developers, deployers, and policymakers to work together. If we are successful in achieving that trust, adoption of AI by consumers and businesses will increase. AI adoption will benefit the users of new services, and it will encourage further development and experimentation in AI and other emerging technology fields, such as quantum and high-performance computing. Commercial successes will provide resources to companies

[8] Testimony of John Miller, Hearing on Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security, Before the U.S. Energy and Commerce Committee (June 14, 2022) *available at* https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-MillerJ-20220614.pdf

[9] We define an **AI system** as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy. This is based on the OECD definition of AI.

that they can invest in AI and other innovations. In that way, **trust is an essential element of a beneficial research and development cycle for technology and the expansion of the AI ecosystem**.

Transparency is a key means by which to achieve that trust. To support those efforts, ITI developed *AI Transparency Policy Principles*.[10] Indeed, ITI members are actively taking steps to build and deploy safe and transparent AI technologies for products and systems. Transparency is paramount for our member companies, particularly when it comes to fostering trust in AI technology. They have placed a premium on these activities. While transparency can take different forms, our companies are working to ensure that users understand when they are interacting with an AI system and broadly how that system works.

In general, transparency can be understood as being clear about how an AI system is built, operates, and functions. When appropriately configured, transparency mechanisms can help to comprehend outputs of an AI system and foster accountability. Transparency is an overarching concept, with both explainability and disclosure falling under this umbrella. In contemplating policy approaches to transparency, we highlight several key considerations that legislators should consider.

First, like with policy approaches to AI generally, **transparency requirements should be risk-based.** It is important to consider the diversity of possible AI use cases and applications, given that the demand for transparency requirements from various users may vary significantly based on the AI application or intended use. Many use cases present little to no risk to the user, and so imposing transparency requirements in such situations will likely add little value to the user and hinder innovation by adding onerous, disproportionate requirements.

Second, in thinking about transparency, **it is important to consider the objective and intended audience.** The target audience at which transparency requirements are directed, including their level of expertise, plays a key role. For example, transparency could be useful to several different audiences (e.g., regulators, consumers, developers, etc.), which will in turn influence the development of potential provisions. Understanding the intended audience will also inform the type of information presented, the way it is presented, and the amount of information presented.

Third, **disclosure can play an important role in facilitating transparency.** AI systems should be disclosed when they are playing a significant role in decision-making or interacting directly with users. In the context of disclosure, language should be plain and clear so that it is understandable to a wide audience. Disclosures should generally include high-level information, such as a topline explanation of how an AI system works, capabilities, and known limitations on performance. Additionally, disclosure should be the responsibility of the deployer to ensure that disclosure and other consumer-facing obligations are met. That said, the developer of the AI system should ensure that terms of sale do not

[10] https://www.itic.org/documents/artificial-intelligence/ITIsPolicyPrinciplesforEnablingTransparencyofAISystems2022.pdf. Transparency is not the only means by which to foster public trust, and so any approach should consider the role that transparency can play, as well as other tools.

prohibit disclosure. Relatedly, we are supportive of information-sharing in the value chain to facilitate cooperation between developers and deployers.

Finally, **Congress should avoid an overly prescriptive approach to transparency and maintain appropriate IP protections.** It is important that transparency requirements allow for flexibility because it may not be appropriate or useful to provide the same type of details in every context or for every target audience.[11] Organizations should have the ability to tailor such information, depending on context, use of, and level or risk associated with the system. Also important is that transparency requirements do not require the disclosure of source code and sensitive IP, or otherwise reveal sensitive individual data**.** Any requirements around transparency should avoid requiring companies to divulge sensitive IP or source code. Disclosure of source code could seriously put at risk trade secrets, undermine IP rights, and contravene widely accepted best practices for digital trade. It could also pose risks to safety and security and allow malicious actors to manipulate an AI system.

D. A pro-innovation policy framework should consider the views and input of all stakeholders.

Both developers and deployers of AI systems should be consulted in the development of policy frameworks, as well as civil society, academia, and companies operating across different sectors. Small, medium, and large companies in all sectors will be using AI to be more efficient and offer better quality services and products, so it is imperative to cast a wide net to obtain a diverse set of perspectives.

Additionally, a pro-innovation policy framework should seek to appropriately delineate the roles and responsibilities of different stakeholders in the AI value chain. **Stakeholders throughout the value chain, including small businesses across a variety of sectors, play a role in the development and deployment of AI in a responsible manner.** As such, responsibilities should reflect the important distinction between developers and deployers and be allocated among actors based on their role and function in the AI value chain.

E. A pro-innovation policy framework should rely upon globally-recognized international standards.

Before adopting new AI regulatory requirements, policymakers should understand the status of international consensus-based standards and the ability of those standards to meet regulatory requirements. AI standards are essential to increase interoperability, harmonization, and trust in AI systems. They can inform AI regulation, practical implementation, governance, and technical requirements. **Without specific standards for risk management processes, such as the measurement and evaluation of models, it will not be possible to implement regulations effectively.** Moreover, regulations that are not aligned with international standards will undermine the leadership of companies doing business in the United States that seek to scale into other jurisdictions that adopt international standards.

[11] Using AI to limit fraud, spam, illegal, or malicious information are some examples of where including technical details or too prescriptive of a disclosure may be inappropriate.

The International Standards Organization and International Electrotechnical Commission have formed a Joint Technical Committee for IT standards, and it has established a subcommittee on Artificial Intelligence (SC 42). That subcommittee has published several AI standards and is working on an Artificial Intelligence Management System (AIMS) standard that will cover processes for the development or use of Al, such as bias, fairness, inclusiveness, safety, security, privacy, accountability, explicability, and transparency.[12] This management system standard will help advance innovation and technology development through structured governance and appropriate risk management. SC 42 currently also has other standards under development, focused on terminology, reference architecture, governance of AI, and trustworthiness. We encourage Congress to consider how standards can address risk management requirements and ensure international harmonization.

III. Conclusion

To lead in AI, the United States needs a pro-innovation policy framework that prioritizes innovation and investment as well as building public trust in AI. Public trust will increase AI adoption by businesses and consumers, and accelerate the flourishing of the AI ecosystem of developers and deployers.

Building public trust through risk management will be critical, and the private sector is already leading in this area, such as through adoption of the NIST AI RMF. The government's role should be limited to addressing critical risks in specific use cases. Where those risks are identified, Congress should evaluate the existing legal and regulatory landscape, and clearly delineate risk areas that are not adequately addressed, before enacting new legislation to address any gaps. Future requirements should be aligned with international consensus standards wherever possible to ensure that risk management is effective and to harmonize the global marketplace for technology.

Thank you, and I look forward to your questions.

[12] See ISO/IEC 42001 Information technology — Artificial intelligence — Management system.