BEFORE THE U.S. HOUSE RESEARCH AND TECHNOLOGY SUBCOMMITTEE

Hearing on "Trustworthy AI: Managing the Risks of Artificial Intelligence"

Testimony of Jordan Crenshaw, Vice President, C_TEC, U.S. Chamber of Commerce

September 29, 2022

Dear Chairman Stevens, Ranking Member Feenstra, and distinguished Research and Technology Committee members. First, thank you for your invitation to come before you today to testify. My name is Jordan Crenshaw, and I am honored to serve as the Vice President of the U.S. Chamber Technology Engagement Center (C_TEC) at the U.S. Chamber of Commerce. C_TEC is the technology hub within the U.S. Chamber, and our goal is to promote the role of technology in our economy and advocate for rational policy solutions that drive economic growth, spur innovation, and create jobs. Today's hearing titled "Trustworthy AI: Managing the Risks of Artificial Intelligence" is a timely and critical discussion, and the Chamber appreciates the opportunity to participate.

The world has quickly entered its fourth industrial revolution, in which the use of technology and artificial intelligence ('AI') is helping propel humanity. However, we are witnessing the benefits of using AI daily, from its value in adapting vaccines to tailor them to new variants to increasing patient safety during procedures like labor and delivery.[1] Artificial intelligence is also rapidly changing how businesses operate. This emerging technology is a tremendous force for good in its ability to secure our networks, expand opportunities for the underserved, and make our communities safer and more prosperous.[2]

America is currently in a race with countries like China to lead in Artificial Intelligence.[3] America's competitors may not respect the same values as our allies, such as individual liberties, privacy, and the rule of law. While the development and deployment of AI have become an essential part of facilitating innovation, this innovation will never reach its full potential and enable the United States to compete without trust. The business community understands that fostering this trust in AI technologies is essential to advance its responsible development, deployment, and use. This has been a core understanding of the U.S. Chamber, as it is the first principle within the 2019 "U.S. Chamber's Artificial Intelligence Principles:

---

[1] https://www.5newsonline.com/article/news/health/northwest-health-introducing-new-technology-to-enhance-maternal-and-fetal-safety/527-9c173d18-c56e-457b-8317-62ebaae93558
[2] https://americaninnovators.com/research/data-for-good-promoting-safety-health-and-inclusion/
[3] https://www.washingtonpost.com/opinions/2022/09/13/artificial-intelligence-ai-high-tech-race-with-china/

Trustworthy AI encompasses values such as transparency, explainability, fairness, and accountability. The speed and complexity of technological change, however, mean that governments alone cannot promote trustworthy AI. The Chamber believes that governments must partner with the private sector, academia, and civil society when addressing issues of public concern associated with AI. We recognize and commend existing partnerships that have formed in the AI community to address these challenges, including protecting against harmful biases, ensuring democratic values, and respecting human rights. Finally, any governance frameworks should be flexible and driven by a transparent, voluntary, and multi-stakeholder process.[4]

AI also brings a unique set of challenges that should be addressed so that concerns over its risks do not dampen innovation and to help ensure the United States can lead globally in trustworthy AI. The U.S. Chamber of Commerce's Technology Engagement Center (C_TEC) shares the perspective with many of the leading government and industry voices, including the National Security Commission on Artificial Intelligence (NSCAI)[5], the National Institute of Standards and Technology (NIST)[6], that government policy to advance the ethical development of AI-based systems, sometimes called "responsible" or "trustworthy" AI, can enable future innovation and help the United States to be the global leader in AI.

This is why we have prioritized the need to build public trust in AI through our continued efforts. The U.S. Chamber earlier this year launched its Artificial Intelligence (AI) Commission on Competition, Inclusion, and Innovation to advance U.S. leadership in using and regulating AI technology.[7] The Commission, led by co-chairs former Congressmen John Delaney and Mike Ferguson, is composed of representatives from industry, academia, and civil society to provide independent, bipartisan recommendations to aid policymakers with guidance on artificial intelligence policies as it relates to regulation, international research, development competitiveness, and future jobs.

Over the past few months, the Commission has heard oral testimony from 87 expert witnesses[8] over five separate field hearings. The Commission heard from individuals such as Jacob Snow, Staff Attorney for the Technology & Civil Liberties Program at the ACLU of Northern California. In his testimony, he told the Commission that the critical discussions on AI are "not narrow technical questions about how to design a product. They are social questions about what happens when a product is deployed to a society, and the consequences of that deployment on people's lives."[9]

Doug Bloch, Political Director at Teamsters Joint Council 7, referenced his time serving on Governor Newsom's Future of Work Commission: "I became convinced that all the talk of

---

[4] https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles
[5] https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf
[6] https://www.nist.gov/artificial-intelligence
[7] www.americaninnovators.com/aicommission
[8] https://americaninnovators.com/aicommission/
[9] https://americaninnovators.com/news/ai-for-all-experts-weigh-in-on-expanding-ais-shared-prosperity-and-reducing-potential-harms/

the robot apocalypse and robots coming to take workers' jobs was a lot of hyperbole. I think the bigger threat to the workers I represent is the robots will come and supervise through algorithms and artificial intelligence."[10]

Miriam Vogel, President and CEO of EqualAI and Chair of NAIAC, also addressed the Commission. She stated "I would argue that it's not that we need to be a leader, it's that we need to maintain our leadership because our brand is trust."

The Commission also received written feedback from stakeholders answering numerous questions that the Commission has posed in three separate requests for information (RFI), which asked questions about issues ranging from defining AI, balancing fairness and innovation,[11] and AI's impact on the workforce.[12] These requests for information outline many of the fundamental questions that we look to address in the Commission's final recommendations, which will help government officials, agencies, and the business community. The Commission is diligently working on its recommendations and will look to release them earlier next year.

While the Chamber is diligently taking a leading role within the business community to address many of the concerns which continue to be barriers to public trust and consumer confidence in the technology, my testimony before you today will look to address the following underlying questions:

- What are the opportunities for the federal government and industry to work together to develop trustworthy AI?
- How are different industry sectors currently mitigating risks that arise from AI?
- How can the United States encourage more organizations to think critically about risks that arise from AI systems, including ways in which we prioritize trustworthy AI from the earliest stages of development of new systems?
- How can the federal government strengthen its role in the development and responsible deployment of trustworthy AI systems?

I. **Opportunities for the Federal Government and Industry to Work Together to Develop Trustworthy AI**

A. *Congress Needs to Pass a Preemptive National Data Privacy Law*

Artificial Intelligence relies upon the data in which it is provided. Particularly sensitive data can be used to determine whether AI systems operate fairly. Many underlying concerns regarding the use of Artificial Intelligence will need to be reassessed should a National Data

---

[10] https://americaninnovators.com/news/ai-for-all-experts-weigh-in-on-expanding-ais-shared-prosperity-and-reducing-potential-harms/

[11] https://americaninnovators.com/wp-content/uploads/2022/04/CTEC_RFI-AIcommission_2.pdf?utm_source=sfmc&utm_medium=email&utm_campaign=&utm_term=RFI+3+-+Workforce+-+20220518&utm_content=5/19/2022
[12] https://uschambermx.iad1.qualtrics.com/jfe/form/SV_cMw5ieLrlsFwUPs

Privacy bill be signed into law as new well-defined rules are put into place. The U.S. Chamber has been at the forefront of advocating for a true *national* privacy standard that gives strong data protections for all Americans equally. For this reason, the Chamber was the first trade association after the passage of the California Consumer Privacy Act to formalize and propose privacy principles and model legislation.[13]

Most central to a national privacy law is the need for true preemption that creates a national standard. A patchwork of fifty different state laws[14] would eliminate the certainty required for data subjects and businesses in compliance and operations. According to a recent report from ITI, a fifty-state patchwork of comprehensive privacy laws could cost the economy $1 trillion and $200 million for small businesses.[15] Recently, the Chamber released findings that nearly 25 percent of small businesses plan to use artificial intelligence and 80 percent of these businesses believe limiting access to data would harm their operations.[16] A state patchwork exacerbates the difficulties these businesses face.

Recently, the House Energy and Commerce Committee reported the American Data Privacy and Protection Act ("ADPPA").[17] Although the ADPPA has many laudable consumer protections like the right to delete, opt out of targeted advertising, as well as data correction and access, there are significant concerns that it could create a new national patchwork and cut off access to data which could improve AI fairness.[18] For example, the bill would only preempt what is covered by the Act and would empower the FTC to bar the collection and use of data.

We encourage stakeholders and Congress to work together to pass a truly preemptive privacy law that enables the use of data to improve AI—not inhibit the deployment of AI.

B. *Support for Alternative Regulatory Pathways Such As Voluntary Consensus Standards*

New regulation is not always the answer for emerging or disruptive technologies. Non-regulatory approaches can often serve as effective tools to increase safety and build trust, and allow for flexibility and innovation. This is particularly applicable to emerging technologies such as artificial intelligence as the technology continues to rapidly evolve.

This is why the Chamber supports the National Institutes of Science and Technology's (NIST) work in drafting the Artificial Intelligence Risk Management Framework (AI_RMF). The

---

[13] https://www.uschamber.com/technology/data-privacy/the-10-principles-of-data-privacy
[14] https://americaninnovators.com/wp-content/uploads/2022/01/CTEC_Privacy2022_HeatMap-1024x791-1.pdf
[15] https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/
[16] https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf
[17] https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf
[18] https://www.uschamber.com/technology/data-privacy/what-should-and-should-not-be-included-in-a-national-privacy-bill

AI RMF is meant to be a stakeholder-driven framework, which is "intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems."

Another example of non-regulation tools is the National Highway Traffic Safety Administration's ("NHTSA") Voluntary Safety Self-Assessments ("VSSA"). More than two dozen AV developers have submitted a VSSA to NHTSA, which have provided essential and valuable information to the public and NHTSA on how developers are addressing safety concerns arising from AVs. The flexibility provided by VSSAs, complemented by existing regulatory mechanisms, provides significant transparency into the activities of developers without compromising safety.

Voluntary tools provide significant opportunities for consumers, businesses, and the government to work together to address many of the underlying concerns with emerging technology while at the same time providing the necessary flexibility to allow the standards not to stifle innovation. These standards are pivotal in the United States' ability to maintain leadership in emerging technology as it is critical to ensuring our global economic competitiveness in this cutting-edge technology.

C. *Stakeholder Driven Engagement*

The U.S. Chamber of Commerce stands by and is ready to assist the government in any opportunity to improve consumer confidence and trust in AI systems. We have always viewed trust as a partnership, and only when government and industry work side by side can that trust be built. The opportunities to facilitate this work are great, but there are essential steps that industry and government can make today.

We asked the American public earlier this year about their perception of artificial intelligence. The polling results were very eye-opening, as there was a significant correlation between the trust and acceptance of AI and an individual's knowledge and understanding of the technology.[19] To build the necessary consumer confidence to allow artificial intelligence to grow for the betterment of all, all opportunities must be taken advantage of for industry and governments to work together in educating stakeholders about the technology.

This is why we appreciate the National Institute of Science and Technology's (NIST) work in drafting the Artificial Intelligence Risk Management Framework (AI_RMF). The AI RMF is meant to be a stakeholder-driven framework. NIST's continued engagement with all stakeholders in the development of the framework is important to develop trust between government and industry. To date, NIST actions include two workshops, with a third workshop scheduled for next month. They have also included three engagement opportunities for stakeholders to provide written feedback on the development, direction, and critique of the AI

---

[19] https://americaninnovators.com/wp-content/uploads/2022/01/CTEC-US-Outlook-on-AI-Detailed-Analysis.pdf

RMF. This engagement by NIST has allowed for the development of trust between industry and the federal government. While we implore NIST and their action on the RMF, it's prudent to highlight that NIST is only one entity within the federal government and that other agencies and regulators should look to the model.

D. Awareness of the Benefits of Artificial Intelligence

At the same time, it is critical that federal agencies do not seek to prescriptively regulate technologies without first establishing a strong public record. The business community has significant concerns about the Federal Trade Commission undertaking rulemaking on privacy, security, and algorithms asking whether it should make economy-wide rules on algorithmic decision systems.[20] First and foremost, the FTC should enable NIST's process to conclude and let Congress speak clearly about how it wants to make policy in artificial intelligence before undertaking general rulemaking. "NIST contributes to the research, standards, and data required to realize the full promise of artificial intelligence (AI) as a tool that will enable American innovation, enhance economic security and improve our quality of life."[21] Therefore, we believe it is essential for NIST to be able to finish the RMF to provide the necessary robust record within the federal government. This is vital, as government agencies such as the FTC ask technical questions.

E. Awareness of the Benefits of Artificial Intelligence

Another excellent opportunity for industry and government to work together is highlighting the benefits and efficiencies of the use of technology within the government. The government's utilization of AI has the ability to lead to medical breakthroughs[22] to help to predict risk for housing and food insecurities.[23] AI is helping our government provide better assistance to the American public, and is becoming a vital tool. The development of these resources does not come in a vacuum, and the majority of these tools are done so in partnership with industry. Highlighting these workstreams and the benefits that they deliver for the American public can assist in fostering trust in technology, as well as build overall consumer confidence in technology use outside of government.

However, this would also require a foundational change in how our government works, which includes addressing the "legacy culture" that has stifled the necessary investment and buildout of 21st-century technology solutions and harnessing data analytics. Congress's passage of the Modernizing Government Technology Act during the 115th Congress was an essential first step in rectifying decades of needed investment. However, this legislation, while important, will not alone fix the problem and would ask Congress to continue to do necessary

---

[20] https://thehill.com/opinion/technology/3621149-the-ftc-needs-a-reminder-that-its-a-regulator-not-a-legislator/

[21] https://www.nist.gov/artificial-intelligence

[22] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/deloitte-analytics/us-ai-institute-goverment-public-services-dossier.pdf

[23] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/deloitte-analytics/us-ai-institute-goverment-public-services-dossier.pdf

oversight within the federal government IT sector so that the essential and sustained investments can be made.

II. How are Different Sectors Adopting Governance Models and Other Strategies to Mitigate Risks that Arise from AI Systems?

AI is a tool and does not exist in a legal vacuum. Policymakers should be mindful that activities performed and decisions aided by AI are often already accountable under existing laws. Where new public policy considerations arise, governments should consider maintaining a sector-specific approach while removing or modifying those regulations that act as a barrier to AI's development, deployment, and use. In addition, governments should avoid creating a patchwork of AI policies at the subnational level and should coordinate across governments to advance sound and interoperable practices.

It's also important to highlight that there is a market incentive for companies to address associated risks with the use of artificial intelligence. Companies to begin with are very risk-averse when it comes to potential legal liabilities associated with their use of the technology. This is why we applaud NIST's development of "Playbook," which is " designed to inform AI actors and make the AI RMF more usable."[24] We believe the playbook will provide a great resource for the business community and industry in helping them evaluate risk.

Every sector will have different risks associated with the use of AI, which is why it is important to maintain a sector-specific approach. However, we believe it's important for policy makers to do necessary oversight to close current legal gaps. For this reason, we would ask policy makers to do necessary oversight of the American COMPETE Act, which requires the U.S. Department of Commerce and Federal Trade Commission ('FTC') to look at different emerging technologies and to conduct a thorough analysis of current standards, guidelines, and policies regarding AI that are implemented by each government agency, as well as industry-based bodies. This important assessment would provide lawmakers and industry with a comprehensive and baseline understanding of relevant regulations that are already in place.

III. How Should the United States Encourage More Organizations to Think Critically about Risks that Arise from AI Systems, Including by Priortiziing Trustworthy AI from the Earliest Stages of Development of New Systems?

The United States has a great opportunity through the development of the NIST AI RMF to provide organizations with a key set of documents that would assist in their ability to think critically about risk. The adaptable voluntary framework would assist companies from big to small in assessing the risk with which they are comfortable and provide guidance on ways to help critical thinking through potential negative externalities which may be associated with its use. That being said, the framework can only assist if it is in the hands of those creating and developing and those who oversee its use. For this reason, we believe that NIST and the

---

[24] https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook-faqs

Department of Commerce should look at ways in which they can reach all different demographics and stakeholders to make them aware of these resources.

Furthermore, we believe further effort should be made by the government to make connections to those small and medium size businesses that usually lack the time and resources to be looking for things like the RMF.

IV. What Recommendations do you Have for how the Federal Government can Strengthen its Role for the Development and Responsible Deployment of Trustworthy AI Systems?

The federal government has the ability to take a leading role in strengthening the development and deployment of artificial intelligence. We believe that the following recommendations should be acted on now.

First, we would advise the federal government to conduct fundamental research in trustworthy AI : The federal government has played a significant role in building the foundation of emerging technologies through conducting fundamental research. AI is no different. A recent report that the U.S. Chamber Technology Center and the Deloitte AI Institute[25] surveyed business leaders across the United States had 70% of respondents indicated support for government investment in fundamental AI research. The Chamber believes that the CHIPS and Science Act was a positive step in the necessary investment, as the legislation authorizes $9 Billion for the National Institutes of Standards Technology (NIST) for Research and Development and advancing standards for "industries of the future," which includes artificial intelligence. Furthermore, wehave been a strong advocate for the National Artificial Intelligence Initiative Act, which was led by Chairwoman Eddie Bernice Johnson and Ranking Member Lucas, which developed the office of the National AI Initiative Office (NAIIO) to coordinate the Federal government's activities, including AI research, development, demonstration, and education and workforce development.[26] We would strongly advise members to appropriate these efforts fully.

Second, we encourage continued investment into Science, Technology, Engineering, and Math Education (STEM).   The U.S. Chamber earlier this year polled the American public on their perception of artificial intelligence. The findings were clear; the more the public understands the technology, the more comfortable they become with its potential role in society. We see education as one of the keys to bolstering AI acceptance and enthusiasm as a lack of understanding of AI is the leading indicator for a push-back against AI adoption.[27]

The Chamber strongly supported the CHIPS and Science Act, which made many of these critical investments, including $200 million over five years to the National Science
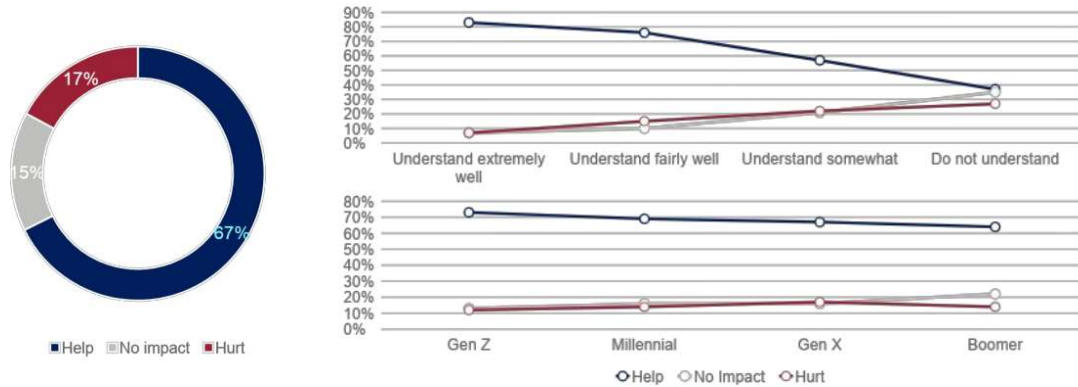
[25] https://www.uschamber.com/technology/investing-trustworthy-ai
[26] https://www.ai.gov/naiio/
[27] https://americaninnovators.com/wp-content/uploads/2022/01/CTEC-US-Outlook-on-AI-Detailed-Analysis.pdf

Foundation (NSF) for domestic workforce build-out to develop manufacture chips, and also $13 Billion to the National Science Foundation for AI Scholarship-for-service. However, the authorization within the legislation is just the start; we now ask Congress to appropriate the funding for these important investments.

Third, the government should prioritize improving access to government data and models: High-quality data is the lifeblood of developing new AI applications and tools, and poor data quality can heighten risks. Governments at all levels possess a significant amount of data that could be used to improve the training of AI systems and create novel applications. When C_TEC asked leading industry experts about the importance of government data, 61% of respondents agree that access to government data and models is important. For this reason, we would encourage policymakers to build upon the success of the OPEN Government Data Act by providing further additional funding and oversight to allow for expanding the scope of the law to include non-sensitive government models as well as datasets at the state and local levels.

Fourth, Increase widespread access to shared computing resources : In addition to high-quality data, the development of AI applications requires significant computing capacity. However, many small startups and academic institutions lack sufficient computing resources, which in turn prevents many stakeholders from fully accessing AI's potential. When we asked stakeholders within the business community about the importance of shared computing capacity, 42% of respondents supported encouraging shared computing resources to develop and train new AI models. Congress took a critical first step by enacting the National AI Research Resource Task Force Act of 2020. Now, the National Science Foundation and the

White House's Office of Science and Technology Policy should fully implement the law and expeditiously develop a roadmap to unlock AI innovation across all stakeholders.

Fifth, Enable open source tools and frameworks : Ensuring the development of trustworthy AI will require significant collaboration between government, industry, academia, and other relevant stakeholders. One key method to facilitate collaboration is through encouraging the use of open source tools and frameworks to share best practices and approaches to trustworthy AI. An example of how this works in practice is the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (RMF), which is intended to be a consensus-driven, cross-sector, and voluntary framework, akin to NIST's existing Cybersecurity Framework, whereby stakeholders can leverage as a best practice to mitigate risks posed by AI applications. Policymakers should recognize the importance of these types of approaches and continue to support their development and implementation

V.   Conclusion

AI leadership is essential to global economic leadership in the 21st century. According to one study, AI will have a $13 trillion impact on the global economy by 2030.[28] Through the right policies, the federal government can play a critical role in incentivizing the adoption of trustworthy AI applications. The United States has an enormous opportunity to transform the economy and society in positive ways through leading in AI innovation as other economies contemplate their approach to trustworthy AI forward on how U.S. policymakers can pursue a wide range of options to advance trustworthy AI domestically and empower the United States to maintain global competitiveness in this critical technology sector. The United States must be the global leader for AI trustworthiness for the technology to develop in a manner that is balanced and takes into account basic values and ethics. The United States can only be a global leader if the administration and Congress work together on a bipartisan basis. We are in a race we can't afford to lose.

---

[28] https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy

Jordan Crenshaw serves as Vice President and leads the day-to-day operations at the U.S. Chamber of Commerce's [Technology Engagement Center](). Crenshaw also directly manages the Chamber's privacy working group which is comprised of nearly 300 companies and trade associations, which developed model privacy legislation and principles. Prior to becoming vice president of C_TEC, he led the Chamber's Telecommunications and E-Commerce Policy Committee, which analyzes federal privacy, cloud computing, broadband, internet, e-commerce, and broadcast policies that impact U.S. businesses.

Before joining the Chamber, Crenshaw served as an attorney focusing on environmental issues and analysis of consumer privacy laws. Crenshaw also worked at McGuireWoods, LLP assisting discovery issues for environmental nuisance, TCPA, and other civil litigation. Crenshaw also served Virginia Senate leadership, the Office of the Attorney General of Virginia, the U.S. Department of Labor Office of Administrative Law Judges, and the National Right to Work Defense Foundation.

Crenshaw earned both his undergraduate degree and Juris Doctor from the College of William and Mary. He is licensed to practice law in Virginia and is a Certified Information Privacy Professional (CIPP/US). He and his wife Molly live in Virginia.