TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

June 12, 2023

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, D.C. 20230

To Whom It May Concern:

TechNet appreciates the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) request for comment on artificial intelligence (AI) system accountability measures and policies. Our members represent many of the leading artificial intelligence (AI) developers, researchers, and deployers of automated systems.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents more than five million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

AI and machine learning (ML) are transformational technologies that have the potential to revolutionize how we live and work and help us solve the most significant challenges of our time. AI and ML can enhance productivity, democratize and expand access to important services, and improve product innovation.

North America currently leads the global AI market — in 2021, the global AI industry was valued at $59.67 billion, and North America accounted for about 43 percent of overall global revenue.[1] However, our international competitors are working quickly to overtake our lead; spending in China's AI industry is forecast to hit $14.75 billion in 2023, accounting for about 10% of the world total.[2] China also currently leads in AI adoption, with 58% of companies deploying AI and 30% considering integration. In comparison, the United States has less than half this adoption rate, with 25% of companies utilizing AI and 43% exploring its potential applications. Industry and government must work together to ensure our nation remains the global technology leader.

TechNet believes that AI systems must be designed, developed, and implemented responsibly and in a way that allows the United States to maintain our lead in innovation

[1] PR Newswire. "$422.37+ Billion Global Artificial Intelligence (AI) Market Size Likely to Grow at 39.4% CAGR During 2022-2028 | Industry." Bloomberg.Com. June 27, 2022. https://www.bloomberg.com/press-releases/2022-06-27/-422-37-billion-global-artificial-intelligence-ai-market-size-likely-to-grow-at-39-4-cagr-during-2022-2028-industry.
[2] Carreon, Miguel, and Michael De La Cruz. "According to IDC'S Forecast, China's AI Market to Exceed US$26 Billion by 2026, Hardware to Make Up 56% of Market." International Data Corporation. May 18, 2023. https://www.idc.com/getdoc.jsp?containerId=prAP50688623.

and builds consumer trust in AI. There are a range of concerns to consider, including but not limited to privacy, transparency, data veracity, bias, security, and workforce. Designers, developers, deployers, and users of AI systems are working to ensure appropriate oversight and accountability; continually monitor and assess the need for improvements related to safety, fairness, and trustworthiness; protect against malicious activity; and address flawed data sets or assumptions. AI regulations should focus on mitigating known risks and providing developers with clear metrics to review their systems.

Utilizing Industry Frameworks and Best Practices

TechNet believes NTIA should promote industry-led processes, standards, and codes of conduct that can help AI stakeholders signal to users that the platform utilizes trustworthy AI systems. This can help users identify which AI tools are reliable and trustworthy and make informed decisions about which tools to use.

Currently, many companies are employing internal processes to assess their AI systems, including internal auditing and impact assessments, which can involve monitoring an AI system for unfair bias, errors, and other issues that could compromise an AI system's reliability and accuracy – and, ultimately, its trustworthiness. These internal audits should be used to improve and update the AI systems accordingly. Throughout the development of AI systems, AI developers work to review the data that is used to train and test their AI models, which can help identify any potential biases or errors in the data.

Many AI stakeholders are applying the NIST AI RMF to review and examine their systems for determining and addressing risk throughout a system's lifecycle. The NIST AI RMF supports AI developers and other stakeholders in this effort by providing a risk-based, voluntary approach to incorporate trustworthiness and accountability benchmarks into the entire lifecycle of an AI system. In addition, the NIST AI RMF appropriately recognizes that the level of risk among different AI use cases can vary significantly.

Similar to the process it used when developing its Cybersecurity and Privacy RMFs, NIST developed its AI RMF in collaboration with key AI researchers, developers, and the broader technology industry. The public-private partnership fostered by NIST and the transparent development process ultimately led to a strong and forward-looking document. We advise that any future AI regulations or standards incorporate the NIST AI RMF as a model for policy development.

Further, TechNet appreciates NIST's launch of the Trustworthy and Responsible AI Resource Center to support AI developers and users in implementing the AI RMF and the development of trustworthy and responsible AI technologies.

The United Nations Guiding Principles (UNGP) on Business and Human Rights offers another example of a framework for stakeholders to develop and operate accountability processes.[3] While the UNGP predates the widespread use of AI technologies, the approach can offer a useful guide. The UNGP does not expect business operations like AI to be impact-free regarding human rights. Instead, businesses should have due diligence processes in place to identify, track, and mitigate any potential human rights issues in their work.

[3] U. N. H. R. O. O. T. H. C. (2011, June 16). *UN Guiding Principles on Business and Human Rights*. Business and Human Rights Resource Centre. Retrieved June 7, 2023, from https://www.business-humanrights.org/en/big-issues/un-guiding-principles-on-business-human-rights/

Scoping

We also want to highlight the importance of clearly defining artificial intelligence. Two key documents that policymakers repeatedly point to, the White House's Blueprint for an AI Bill of Rights and NIST's AI Risk Management Framework, utilize different definitions of AI. While both documents offer voluntary, non-binding guidance, these differing definitions — both issued by the same administration — can send confusing messages to businesses that develop and deploy AI. In its Request for Comment, NTIA points to both documents, exacerbating this uncertainty. We advise the use of the NIST AI RMF's definition[4] of an AI system for two reasons: 1) the RMF was developed through close coordination with the experts from the AI community, and 2) it was adapted from existing AI industry definitions.[5] Adopting the NIST AI RMF definition across government will help provide greater clarity for the public's understanding of AI systems.

Independent Assessments

TechNet members believe that it is premature to mandate independent third-party auditing of artificial intelligence systems. NTIA's RFC states that "… it is imperative that those performing AI accountability tasks are sufficiently qualified to provide credible evidence that systems are trustworthy." TechNet is concerned that there is not currently a well-established credentialing regime for AI auditing, such as exists for financial services. In some cases, particularly with sophisticated AI developers that have robust responsible AI systems, their internal auditing programs far surpass third-party options. Mandating an independent audit before the market reaches maturity could open AI systems to national security threats, trade secrets theft, and inaccurate audit reports.

Manual and Automated Systems

The NTIA RFC states that a goal of an AI assessment could be that "[t]here are adequate human alternatives, consideration, and fallbacks in place throughout the AI system lifecycle." TechNet agrees that developers should have a thorough review of the resiliency of their systems and contingency considerations; however, requiring a "manual" version of all automated systems is neither feasible nor practical.

Requiring an overly broad "opt-out" feature to direct users to manual systems will ultimately discourage the development of trustworthy AI by disincentivizing AI research and deployment. If companies are also required to offer a manual system in broad circumstances, there will be less of a compelling business case to innovate and develop advanced responsible AI technologies. This in turn, will depress American AI development when the stakes for global leadership in AI innovation are at their highest and could cause the United States to not only cede our role as the world's global technology leader but to provide a pathway for foreign adversaries to gain that mantle.

Many interfaces on the internet are run using automated systems, and requiring an "opt-out" option in all instances would necessitate building duplicative sites that will often not be able to provide either the same amount nor degree of services that an AI-powered site

[4] The AI RMF defines an AI system as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.
[5] OECD Recommendation on AI:2019; ISO/IEC 22989:2022.

offers. It also could lead to greater inefficiencies for consumers, increased cybersecurity risks, and hamper access to digital services. TechNet believes that requirements for manual alternatives should be based on the known risks of each use case. We are concerned that manual options may not be feasible or effective for all scenarios where AI is utilized.

The Need for a Federal Privacy Law

We also want to take this opportunity to highlight the need for a federal privacy law, which would allay concerns about the harms to consumer privacy from the use of AI. In the RFC, NTIA mentions that a goal of AI assessments could include a review that "the AI system protects privacy." The passage of a federal consumer data privacy law should precede AI-focused legislation, as privacy legislation would apply to and mitigate some risks to consumers stemming from using AI systems. A federal privacy law will help consumers understand their rights relating to the data used to inform automated systems and will assist developers in knowing their liability when managing large datasets. By having a clear national framework, we can help build trust in AI systems deployed across the United States utilizing the same standards when it comes to consumer privacy.

TechNet has long urged policymakers on Capitol Hill to craft a federal privacy law that protects consumers and provides businesses with certainty about their responsibilities. The current and growing landscape of state privacy laws has created a patchwork of laws, standards, and obligations that confuse consumers and hurt our nation's innovators, especially our small and medium-sized businesses. Costs from 50-state privacy laws could exceed $1 trillion over ten years, with at least $200 billion being paid by small businesses.[6] A federal privacy law will help consumers better understand their privacy rights and avoid the confusion resulting from differing policies state-to-state.

Congressional action is the best approach to a federal privacy law because Congress can expressly preempt state laws and ensure that authorities with relevant expertise are responsible for enforcement. This is also an issue of bipartisan interest; a *Morning Consult* survey found that 86 percent of Democrats and 81 percent of Republicans said Congress should make privacy a "top" or "important" priority.[7] TechNet is pleased that Congress has recently demonstrated a willingness to address this challenge and is making real progress towards passing bipartisan federal privacy legislation. We are hopeful this momentum continues and culminates in a uniform, coherent national privacy framework.

Conclusion

The federal government must avoid blanket prohibitions and overly prescriptive requirements on AI, ML, or other forms of automated decision-making. With the increased interest in AI due to the popularity of publicly accessible generative AI systems, there has been a discussion of policies that would inhibit the United States' ability to continue leading in this important technology. These suggestions have included a proposal to place a six-

[6] Castro, Daniel, Luke Dascoli, and Gillian Diebold. "The Looming Cost of a Patchwork of State Privacy Laws." Information Technology and Innovation Foundation. January 24, 2022. https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.
[7] Sabin, Sam. "States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data." Morning Consult. April 27, 2021. https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/?mkt_tok=ODUwLVRBQS01MTEAAAF8tGX5mckivVTqDBnO2P6uk8SwNzpikG6iODLZhMUSXoCz_rBTKebgwsCEXL0Ix0rfXmhJBFrFEj02zoCiQuwy_kXz5hl02m-CJADuAAR7j8c.

month ban on AI development,[8] which would merely lend additional time to foreign competitors to gain an advantage over American AI development. Any restrictions on automated decisions should be risk-based and focused on responding effectively to specific actual harms while allowing for advancements in technology and innovation. A risk-based regulation allows for application across industries and will help future-proof policies as this technology continues to develop. TechNet advocates for requirements of manual alternatives to be tailored to the known risks associated with each specific use case. Furthermore, TechNet strongly urges the development of AI regulations in collaboration with sector experts who possess deep knowledge of the use cases where the technology is being deployed. This collaboration will help ensure that regulators have the necessary expertise to effectively address the unique challenges presented by each sector's AI applications.

It is important to note that the use of AI in furtherance of unlawful behavior is already prohibited and is actionable under existing laws, without the need for AI-specific regulation. For example, many existing anti-discrimination laws apply to AI models in important areas, including housing, employment, and financial services (i.e., the *Fair Housing Act*, Title VII of the *Civil Rights Act of 1964*, *National Labor Relations Act,* and the *Equal Credit Opportunity Act*). Additional oversight in these areas would be unnecessarily duplicative and may create inconsistent or conflicting standards.

We look forward to working with you on AI policy and appreciate the opportunity to discuss this innovative technology. Thank you for your consideration of our perspective on this important issue.

Sincerely,

Carl Holshouser

Carl Holshouser
Senior Vice President

[8] Future of Life Institute. "Pause Giant AI Experiments: An Open Letter." Future of Life Institute. March 22, 2023. https://futureoflife.org/open-letter/pause-giant-ai-experiments/.