



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | [@TechNetUpdate](https://twitter.com/TechNetUpdate)

July 7, 2023

Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, D.C. 20504

To Whom It May Concern:

TechNet appreciates the opportunity to respond to the Office of Science and Technology Policy's (OSTP) request for information on developing a National AI strategy. Our members represent many of the leading artificial intelligence (AI) and automated systems developers, researchers, deployers, and users.

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 4.5 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%

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>.

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 its lead in innovation and builds user trust and confidence 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 throughout the lifecycles; 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 to identify and mitigate novel and emerging risks.

Existing Legal Protections

It is important to note that the use of AI in furtherance of unlawful behavior is already prohibited and actionable under existing laws, even in the absence of AI-specific regulation. For example, many existing anti-discrimination laws apply to AI models in important areas, including education, healthcare, employment, housing, credit, policing and criminal justice, and access to goods and services.³

Several federal leaders have stated their intent to use existing laws to regulate AI; for example, on April 25, the Consumer Financial Protection Bureau, the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission, and the Federal Trade Commission issued a joint statement outlining how their existing enforcement authorities apply to automated systems.⁴ In addition, National Labor Relations Board (NLRB) General Counsel Jennifer Abruzzo has stated that she will "... apply the [National Labor Relations] Act to protect employees from intrusive electronic monitoring and automated management practices...".⁵ Additional oversight in these areas should not be unnecessarily duplicative or create inconsistent or conflicting standards.

³ Several existing enforcement statutes were outlined in the National AI Advisory Committee's Year One Report: *Civil Rights Act of 1964, Equal Educational Opportunities Act, Americans with Disabilities Act, Individuals with Disabilities in Education Act, Genetic Information Nondiscrimination Act, Immigration and Nationality Act's Anti-Discrimination Provision, Fair Housing Act, Equal Credit Opportunity Act, Violent Crime Control and Law Enforcement Act, and the Omnibus Crime Control and Safe Streets Act.*

⁴ Chopra, Rohit, Kristen Clarke, Charlotte Burrows, and Lina Khan. "JOINT STATEMENT ON ENFORCEMENT EFFORTS AGAINST DISCRIMINATION AND BIAS IN AUTOMATED SYSTEMS." FTC.Gov. April 25, 2023. <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/joint-statement-enforcement-efforts-against-discrimination-bias-automated-systems>.

⁵ Office of Public Affairs. "NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices." National Labor Relations Board. October 31, 2022. <https://www.nlr.gov/news-outreach/news-story/nlr-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and>.

TechNet members comply with existing legal requirements, including laws protecting privacy and preventing discrimination. The use of AI applications falls within the scope of these legal protections. Accordingly, TechNet members are designing, developing, deploying, and using AI technology cautiously and only after rigorously assessing the benefits and risks of implementation.

Utilizing Industry Frameworks and Best Practices

TechNet believes the White House should promote technical standards and codes of conduct developed through industry-led processes 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 review the data 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 frameworks, 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.

TechNet also 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. NIST's recently announced plans to convene a public working group on generative AI will further these important objectives.⁶

⁶ National Institute of Standards and Technology. "Biden-Harris Administration Announces New NIST Public Working Group on AI." June 22, 2023. <https://www.nist.gov/news-events/news/2023/06/biden-harris-administration-announces-new-nist-public-working-group-ai>.

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.⁷ While the UNGP predates the widespread use of AI technologies, the approach can offer a useful guide. The UNGP does presume that business operations like AI will 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.

Supporting the NAIRR

TechNet is supportive of developing and funding the National AI Research Resource (NAIRR) to help ensure America continues to lead on AI R&D and bring the benefits of this innovative technology to every zip code. The NAIRR will look to establish a "... widely accessible AI research cyberinfrastructure that brings together computational resources, data, testbeds, algorithms, software, services, networks, and expertise... [which] would help democratize the AI research and development (R&D) landscape in the United States for the benefit of all."⁸ By leveraging our nation's existing artificial intelligence research resources, the NAIRR will empower small- and medium-sized enterprises and academics to discover next-generation automated systems.

Need for an AI Workforce

In its final report, the National Security Commission on Artificial Intelligence (NSCAI) stated that "the artificial intelligence competition will not be won by the side with the best technology. It will be won by the side with the best, most diverse, and tech-savvy talent... Digital expertise is the most important requirement for government modernization, but few parts of government have adequately invested in building a digital workforce."⁹ NSCAI was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to comprehensively advance AI technologies to meet the national security and defense needs of the United States, and we agree with their focus that a modern American AI workforce is crucial for our continued international leadership.¹⁰

We encourage the White House to utilize best practices and materials developed by the NAIRR to support educators. The NAIRR Task Force's report envisions that "educators should have new, readily available options for incorporating AI tools and training materials that support student learning in AI, including the ethics of AI.

⁷ 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/>

⁸ National Artificial Intelligence Research Resource Task Force. "Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem: An Implementation Plan for a National Artificial Intelligence Research Resource." March, 2021. <https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf>.

⁹ National Security Commission on Artificial Intelligence. "Final Report." June 27, 2023. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top.

¹⁰ P.L. 115-232

Students should gain new and early exposure to AI tools and methodologies that transform their understanding; increase their interest in AI and other science, technology, engineering, and mathematics (STEM) fields; and broaden engagement across the full pool of talent to help build a strong and diverse future AI innovation ecosystem.” Many TechNet members are currently providing upskilling opportunities for individuals looking to enter the innovation economy, and we would like to remain partners with federal and state governments to design effective workforce programs.

TechNet has also been a longtime supporter of the creation of a National Digital Reserve Corps. A National Digital Reserve Corps aims to bridge federal government needs and private sector capabilities by establishing a program within the General Services Administration (GSA) to manage a reserve of individuals with the credentials to address the digital and cybersecurity needs of Executive Agencies across the federal enterprise both before and when cyber incidents arise. This proposal was supported in the NSCAI’s final report and by the National Artificial Intelligence Advisory Committee (NAIAC) in its Year One Report.¹¹ We believe this kind of creative thinking and public-private partnership can buttress the American government’s workforce needs and support ongoing federal government modernization efforts.

Independent Assessments

TechNet members believe it is premature to mandate independent third-party auditing of AI systems. TechNet is concerned that there is no well-established credentialing system for AI auditing, such as that exists for financial services or even cybersecurity. A robust credentialing system requires credentialing standards which have not been established; these standards would require a high level of understanding of AI systems, risks, approaches, and use cases. Mandating an independent audit before the market reaches maturity could open AI systems to national security threats, trade secrets theft, and inaccurate audit reports.

In some cases, particularly with sophisticated AI developers that have robust responsible AI systems, internal auditing programs far surpass third-party options. Internal audits take into consideration the specific use case of the automated system and measure it against relevant standards for its application and are thereby able to provide more thorough reviews than a standard third-party audit would.

Manual and Automated Systems

There have been policy proposals for mandating manual duplications of automated systems for users to “opt-out” to. TechNet agrees that developers should have a thorough review of the resiliency of their systems and contingency considerations;

¹¹ NAIAC. "National Artificial Intelligence Advisory Committee (NAIAC) Year One Report." May 1, 2023. <https://www.ai.gov/wp-content/uploads/2023/05/NAIAC-Report-Year1.pdf>.

however, requiring a “manual” version of all automated systems is neither technically 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 exceed U.S. capabilities.

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 offers. It also could lead to greater inefficiencies and costs 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.

Improved Cybersecurity

Automated tools are also being deployed to actively protect American devices from cybersecurity threats. With fast-evolving cyberattacks and the multiple devices individuals utilize today, AI and machine learning (ML) can help keep cybercriminals at bay, automate threat detection, and respond more effectively than conventional software-driven or manual techniques. By using sophisticated algorithms, automated systems are being trained to detect malware, run pattern recognition, and detect even the most minute behaviors of malware or ransomware attacks before they enter the system. Ransomware attackers extorted at least \$765.5 million from victims in 2021, and the actual number is expected to be much higher.¹² Many of these cybercriminals are working on behalf of America’s hostile competitors. Earlier this year, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory on how the Democratic People’s Republic of Korea’s (DPRK) state-sponsored ransomware was targeting America’s healthcare systems.¹³ These extorted funds then go on to support the development of additional malicious technologies to target American and allied entities. Automated tools can help protect public and private institutions, Americans’ personal data, and our economy writ large from cyber criminals.

¹² Chainanalysis Team. "Ransomware Revenue Down As More Victims Refuse to Pay." January 19, 2023. <https://blog.chainanalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/>.

¹³ CISA Media Relations. "#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities." February 9, 2023. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a>.

Environmental Benefits

Through enhanced monitoring and optimization, AI can aid humans in predictive, proactive, and reactive action against climate change. By increasing efficiency and optimizing performance, the use of AI to create shared, electric, and driverless transportation may reduce emissions by 50 percent by 2050 “through route and traffic [optimization], eco-driving algorithms, programmed “platooning” of cars to traffic, and autonomous ride-sharing services.”¹⁴

AI can be used to optimize the electric grid — “[predicting] the demand and supply for renewables across a distributed grid, [improving] energy storage, efficiency, and load management, [assisting] in the integration and reliability of renewables and [enabling] dynamic pricing and trading, creating market incentives.”¹⁵ On a more granular scale, AI can be used in households and businesses to monitor and optimize electricity usage, turning off lights or heat.¹⁶ AI can also be used to monitor and mitigate the current impacts of climate change more efficiently. Automated tools are currently being used to accurately monitor and report methane emissions, helping companies and governments alike.¹⁷ Major utility providers are already deploying these modern tools.¹⁸

Experts predict AI could precipitate scientific breakthroughs to help combat climate change. For example, DeepMind co-founder, Demis Hassabis, has suggested that in materials science, a descendant of AlphaGo Zero could be used to search for a room-temperature superconductor — a hypothetical substance that allows for incredibly efficient energy systems.¹⁹ The application of AI to greatly reduce the lead time needed to develop new materials or optimize the physio-chemical characteristics of existing materials is unleashing a renaissance in materials science that will help address sustainability objectives through reduced material use and improved recycling. With the right clean energy sources to power data farms (offsetting AI’s carbon footprint), AI can be a critical tool in the effort to reduce greenhouse gases.²⁰

¹⁴ “Artificial Intelligence’s Environmental Costs and Promise,” Council on Foreign Relations, accessed June 27, 2023, <https://www.cfr.org/blog/artificial-intelligences-environmental-costs-and-promise>; “8 Ways AI Can Help Save the Planet,” *AI for Good* (blog), January 31, 2018, <https://aiforgood.itu.int/8-ways-ai-can-help-save-the-planet/>; Kat Kerlin, “You Say You Want a Transportation Revolution? How About Three of Them?,” UC Davis, May 2, 2017, <https://www.ucdavis.edu/news/you-say-you-want-transportation-revolution-how-about-three-them-0>.

¹⁵ “8 Ways AI Can Help Save the Planet,” *AI for Good* (blog), January 31, 2018, <https://aiforgood.itu.int/8-ways-ai-can-help-save-the-planet>.

¹⁶ “How Artificial Intelligence Is Helping Tackle Environmental Challenges,” UNEP, November 7, 2022, <http://www.unep.org/news-and-stories/story/how-artificial-intelligence-helping-tackle-environmental-challenges>.

¹⁷ “Artificial Intelligence’s Environmental Costs and Promise.”

¹⁸ “Duke Energy’s AI Methane Detection Platform | Accenture,” accessed June 27, 2023, <https://www.accenture.com/us-en/case-studies/utilities/duke-energy-powers-ai-platform-summary>; “Global Alarm System Watches for Methane Superemitters,” accessed June 27, 2023, <https://www.science.org/content/article/global-alarm-system-watches-methane-superemitters>.

¹⁹ “8 Ways AI Can Help Save the Planet.”

²⁰ “Artificial Intelligence’s Environmental Costs and Promise.”

Scoping

We want to encourage the use of a consistent and clear definition for artificial intelligence. Policymakers repeatedly point to two key documents, the White House's Blueprint for an AI Bill of Rights and NIST's AI Risk Management Framework, which 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. We advise the use of the NIST AI RMF's definition²¹ 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.²² Adopting the NIST AI RMF definition across the government will help provide greater clarity for the public's understanding of AI systems.

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 harm to consumer privacy from the use of AI. In his 2022 State of the Union speech, President Biden spoke on the importance of strengthening privacy protections, and TechNet believes the moment is ripe for this key legislation.²³ The passage of a federal consumer data privacy law should be a part of or pass concurrently with AI-focused policy, 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. A clear national framework will build trust in AI systems by ensuring that the same consumer privacy standards are used for all AI systems deployed across the United States.

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 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 small and medium-sized businesses. Costs from 50 state privacy laws would exceed \$1 trillion over ten years, with at least \$200 billion being paid by small businesses.²⁴ A federal privacy law will help consumers better understand their privacy rights and avoid the confusion resulting from differing policies state-to-state.

²¹ 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.

²² OECD Recommendation on AI:2019; ISO/IEC 22989:2022.

²³ Biden, Joseph R. "2022 State of the Union Address." Speech, Washington, D.C., 2022. Accessed June 6, 2023. <https://www.whitehouse.gov/state-of-the-union-2022/>

²⁴ 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/>.

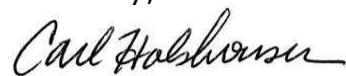
Congressional action is the best approach to a federal privacy standard because Congress can expressly preempt state laws and ensure that authorities with relevant expertise are responsible for enforcement. This is an issue of bipartisan interest; a *Morning Consult* survey found that 86 percent of Democrats and 81 percent of Republicans said Congress should make privacy a “top” or “important” priority.²⁵ TechNet is pleased that Congress has recently demonstrated a willingness to address this challenge and is making real progress toward 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-month ban on AI development,²⁶ 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. 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 industry 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 all AI applications.

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
Senior Vice President

²⁵ 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=ODUwLVRBQS01MTEAAAF8tGX5mckivVTqDBnO2P6uk8SwNzpkG6iODLZhMUSXoCz_rBTKebgwsCEXLOIx0rfXmhJBFrFEj02zoCiQuwy_kXz5hI02m-CJADuAAR7j8c.

²⁶ 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/>.