TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

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

June 29, 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 automated systems use in the workplace. 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 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% 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.

[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.

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 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.

Existing Legal Protections

It is important to note that the use of AI in furtherance of unlawful behavior is already prohibited and is 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 employment and the workplace (i.e., Title VII of the *Civil Rights Act of 1964*, the *National Labor Relations Act,* and the *Americans with Disabilities Act*).

Several federal leaders have stated their intent to use existing laws to regulate AI; for example, 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 electric monitoring and automated management practices…".[3] 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] Additional oversight in these areas should not be unnecessarily duplicative or create inconsistent or conflicting standards.

TechNet members comply with existing legal protections, including existing privacy and anti-discrimination laws. The use of automated technologies in the workplace does not fall outside of the scope of these legal protections. Accordingly, TechNet members adopting AI technology do so cautiously and only after rigorously assessing the benefits and risks of implementation.

Enhancing Safety

Several TechNet members use automated tools to provide navigation, routing, and transportation safety assistance to users, independent contractors, and employees. NHTSA projects that an estimated 42,915 people died in motor vehicle traffic crashes in 2021, a 10.5% increase from the 38,824 fatalities in 2020. This projection is the

[3] 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.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and.
[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.

highest number of fatalities since 2005 and the largest annual percentage increase in the Fatality Analysis Reporting System's history.[5] TechNet agrees with Transportation Secretary Pete Buttigieg, who stated that "[t]he rising fatalities on our roadways are a national crisis; we cannot and must not accept these deaths as inevitable."[6]

Many members utilize telematic services to improve the efficiency and safety of their fleets. Research has shown that these services can decrease risky driving practices. Cambridge Mobile Telematics, the world's largest telematics service provider, has shown that its Hard Brake Alerts have helped reduce hard braking by 14%, and that of the drivers who have experienced Hard Break Alerts, 72% said the alert positively influenced their driving behaviors. Hard Brake Alerts are also an optional feature — drivers can opt out at any time.[7] As tens of thousands of Americans continue to die on our roadways every year, companies are working to deploy tools to keep their employees and independent contractors safe as they go about their work.

AI-empowered technologies can also keep employees safe from incidents beyond the roadways. Samdesk, a global crisis detection platform, works with several companies to provide Real-Time Safety Alerts in the event of emergencies.[8] This system reviews public data sets to spot disruptive events and send early warning alerts and insights, often ahead of traditional news and crisis monitoring tools. This can allow companies to alert employees, independent contractors, and users about the incident, suspend operations, avoid the impacted area, and stay out of harm's way.

Improved Cybersecurity

Automated tools are also being deployed to actively protect employees' devices from cybersecurity threats. With fast-evolving cyberattacks and the multiple devices individuals now utilize today, AI and machine learning (ML) can help to 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 real number is expected to be much higher.[9] 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 (DPRK) state-sponsored ransomware

[5] NHTSA Media. "Newly Released Estimates Show Traffic Fatalities Reached a 16-Year High in 2021." NHTSA. May 17, 2022. https://www.nhtsa.gov/press-releases/early-estimate-2021-traffic-fatalities.
[6] NHTSA Media. "NHTSA Data Estimates Indicate Traffic Fatalities Continued to Rise at Record Pace in First Nine Months of 2021." NHTSA. February 1, 2022. https://www.nhtsa.gov/press-releases/traffic-fatalities-estimates-jan-sept-2021.
[7] Cambridge Mobile Telematics. "Cambridge Mobile Telematics Launches Solution to Reduce Crash Frequency." Cmtelematics.Com. September 20, 2022. https://www.cmtelematics.com/news/cambridge-mobile-telematics-launches-solution-to-reduce-crash-frequency/.
[8] Samdesk. "Samdesk Partners with DoorDash to Help Keep Dashers Safe." January 29, 2023. https://www.samdesk.io/blog/samdesk-partners-with-doordash-to-help-keep-dashers-safe.
[9] Chainanalysis Team. "Ransomware Revenue Down As More Victims Refuse to Pay." January 19, 2023. https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/.

was targeting America's healthcare systems.[10] 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 cybercriminals.

Supporting Employees with Advanced Tools

Automated systems are being deployed in workplaces across the country to help free employees from rote and inefficient tasks so they can focus on creative outputs. Several of our members utilize automated tools to assist with scheduling, which can ensure more experienced managers are on the same shift as new employees for mentoring, coordinating predictive maintenance for equipment, or when additional orders for needed supplies should go out. While a human could organize these services, by automating these operations, employees are able to make decisions more quickly and go about their workday in a more efficient manner. We are seeing that AI-driven tools enable larger, more integrated teams because entities can coordinate and collaborate more effectively. According to a study by MIT Sloan, employees that are empowered by AI feel more competent in their roles, more autonomous in their actions, and more connected to their work, colleagues, partners, and customers. Only 8% of the global survey respondents were less satisfied with their jobs because of AI.[11] When reviewing the impact of automated tools in the workplace, TechNet urges OSTP to consider the wider context of these systems' impact on employees' well-being in their careers.

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. We advise the use of the NIST AI RMF's definition[12] 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.[13] Adopting the NIST AI RMF definition across the government will help provide greater clarity for the public's understanding of AI systems.

[10] 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.
[11] S. Ransbotham, D. Kiron, F. Candelon, S. Khodabandeh, and M. Chu, "Achieving Individual — and Organizational — Value With AI," *MIT Sloan Management Review* and Boston Consulting Group, November 2022
[12] 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.
[13] OECD Recommendation on AI:2019; ISO/IEC 22989:2022.

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 the RFI, OSTP makes repeated mention of the importance of protecting Americans' privacy. 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. 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.[14] 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.[15] 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

[14] 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/.

[15] 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.

included a proposal to place a six-month ban on AI development,[16] 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.

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

[16] 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/.