

Comments of Reason Foundation on the Development of an Artificial Intelligence (AI) Action Plan

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.

Introduction

On behalf of Reason Foundation, we respectfully submit these comments in response to the Networking and Information Technology Research and Development (NITRD) National Coordination Office's (NCO) request for information on the Development of an Artificial Intelligence (AI) Action Plan. Reason Foundation is a national 501(c)(3) public policy research and education organization with expertise across a range of policy areas, including emerging technology.

We applaud President Trump's Executive Order (E.O.) 14179, Removing Barriers to American Leadership in Artificial Intelligence, signed on January 23, 2025. We shared President Trump's concern regarding former President Biden's E.O. 14110, and we support the decision to revoke it in E.O. 14148. President Trump's E.O. 14179 properly focuses on innovation and global competitiveness to keep the United States at the cutting edge of this critical new technology.

The United States is the world's leader in both innovation and the deployment of new technologies because of its dynamic market economy. Artificial intelligence (AI) promises to be among the most important technological revolutions in recent history, and the importance of President Trump renewing the nation's commitment to free markets and bold innovation in E.O. 14179 cannot be overstated.

AI is the type of foundational technology where new ideas build on each other, opening innovative paths that are difficult to foresee in advance, and counterproductive to regulate using knowledge that will quickly become obsolete. We agree with Vice President Vance that "AI will have countless revolutionary applications in economic innovation, job creation, national security, healthcare, free expression, and beyond." Free markets are not just the best way to realize this future, they are the only way to realize it.

To assist in the Administration's development of an AI Action Plan, we submit comments on several key policy areas important to continued AI growth: avoiding overregulation, data access, security, and free speech.

Avoiding Overregulation and Encouraging Innovation

President Trump's E.O. 14179 reflects a decisive shift toward a light-touch regulatory approach to AI development and deployment in the United States.¹ This policy direction focuses on prioritizing innovation and global competitiveness while reversing regulations that could be burdensome to AI development. We see the development of the AI Action Plan as a key opportunity for the Trump Administration to work alongside developers and deployers of AI to create a clear and concise framework to best encourage innovation.

Among the most important steps the AI Action Plan can take is discouraging overregulation of AI. As Vice President J.D. Vance noted in his February 11, 2025 remarks at the Artificial Intelligence Action Summit in Paris, governments frequently respond to new technologies by being "too self-conscious, too risk-averse." When governments regulate new technology too early, they often completely cut off whole directions for development without knowing it. Innovation is a costly and uncertain process, for which people and firms freely competing in the private sector is essential.

Revoking former President Biden's E.O. 14110 was an important step in this direction. In that case, fears about outcomes like discrimination motivated premature and burdensome regulation. Importantly, the United States already has numerous laws and regulations prohibiting discriminatory conduct. We will not know if or how these laws should be modified until the technology develops further.

The Action Plan should adopt a similar recommendation that would be applied across federal departments and use cases for AI. Federal agencies should clarify how existing laws apply to AI technology rather than introducing duplicative or overly burdensome new regulations. Many existing legal frameworks can be adapted to address emerging AI challenges, reducing the need for entirely new regulations. This approach not only minimizes compliance burdens for businesses but also ensures that regulations remain flexible enough to accommodate the rapid evolution of AI technologies.

The Action Plan should also seek to make recommendations that are responsive to the many diverse use cases and industries that AI promises to impact. Different industries use AI in unique ways, and a one-size-fits-all regulatory approach may fail to address sector-specific risks and opportunities. For instance, health care applications of AI require stringent privacy protections due to sensitive patient data, while financial services, fairness and anti-discrimination concerns could come to the forefront in credit scoring algorithms.² The Action Plan should encourage

¹ Exec. Order 14179, 90 Fed. Reg. 8741 (Jan. 31, 2025).

² Yu-Hao Li et al., "Innovation and challenges of artificial intelligence technology in personalized healthcare," *Scientific Reports*, Vol. 14, No. 18994, August 2024.

agencies to make use of technical expertise in the private sector for knowledge and tools needed to craft effective policies tailored to their domains.

By taking stock of laws and regulations that already apply to AI, determining general and industry-specific legal issues that may arise, and learning from ongoing innovation in the private sector, federal agencies can move toward consistent, clear, and flexible AI policy that will encourage rather than stifle innovation.

Promoting Secure Access to Data for AI Models

Former President Biden's E. O. 14110 sought to scrutinize how personal data might be used in training datasets, no matter if it was private or publicly available.³ In keeping with President Trump's goal of promoting AI innovation, the Action Plan should encourage the removal of barriers to accessing and utilizing public data for the training of AI models.⁴ Unrestricted access to public information is crucial for maintaining the United States' global leadership in AI technology. This approach aligns with the Administration's goal of maintaining American AI leadership worldwide.

Both publicly available data and private data are necessary for AI models' continued improvements. Any standard on data collected for AI models should adopt a clear distinction between publicly available and private personal data. Publicly available data includes information that is accessible to the general public, often through government records, public websites, or other open sources. In contrast, private personal data is information that is not intended for public access and is typically collected directly from individuals with an expectation of confidentiality.

Access to publicly available data directly impacts AI systems' quality, functionality, and overall performance.⁵ It also enables substantial cost and time efficiencies for researchers, entrepreneurs, and government agencies. By eliminating the need to collect, aggregate, and store data from scratch, these stakeholders can focus their resources on problem-solving and innovation. This accelerates the development of new AI models and enables the creation of diverse applications across multiple sectors, from health care and housing to economic development and national security.

³ Exec. Order 14110, 88 Fed. Reg. 75191 (Nov. 1, 2023).

⁴ Exec. Order 14179.

⁵ Spencer Ferguson and Patricia M. Tille, "Public Datasets: A Foundation to Artificial Intelligence in Health Care," *Clinical Laboratory Science*, Vol. 37, No. 2, April 2024.

Open data fosters innovation by promoting higher quality decision-making, increasing data-driven accountability, and supporting global advancements in AI. Government agencies can use these AI tools leveraging open data to enhance the efficiency, accessibility, and effectiveness of services.⁶ For instance, machine learning algorithms can process weather information to provide timely insights to farmers, or AI can simplify tax filing processes for citizens.⁷ The combination of open data and AI holds great promise for improving government efficiency, reducing fraud risks, and enhancing security in key economic sectors.

The research community benefits immensely from public datasets, as these enable the training of predictive models that create value for both public and private sectors. Government healthcare data, for example, can contribute to improving existing treatment options and even aid in the development of novel cures.⁸ By making information freely available for people and entities to use, reuse, and consume, open data, more people can contribute to the United States' AI development and keep the country at the top of such development.

While access to personal data is also important to AI development, this can raise serious privacy concerns. The AI Action Plan should encourage agencies to work together and with the private sector to keep data secure as technology continues to evolve. Maintaining data security both reduces the risk of personal information being leaked and helps create avenues for more secure AI development in the future. The federal government can collaborate with industry to enhance data security. The National Institute of Standards and Technology (NIST) enhances data security by providing structured guidelines in its Cybersecurity Framework (CSF) and AI Risk Management Framework (AI RMF) for managing risks across traditional information technology infrastructure and AI systems, respectively.⁹ The CSF focuses on foundational protections like encryption and access controls, while the AI RMF addresses unique AI risks such as data privacy. These two frameworks help ensure comprehensive security through proactive risk management and regulatory alignment.

⁶ “Open data and AI: A symbiotic relationship for progress,” Publications Office of the European Union, June 9, 2023, <https://data.europa.eu/en/publications/datastories/open-data-and-ai-symbiotic-relationship-progress>.

⁷ Lax Gopisetty, “The Beneficial Impact of AI in Public Services,” RTInsights, March 7, 2025, <https://www.rtinsights.com/the-beneficial-impact-of-ai-in-public-services/>.

⁸ Kornelia Batko and Andrzej Ślęza, “The use of Big Data Analytics in healthcare,” *Journal of Big Data*, Vol. 9, No. 1, January 2022.

⁹ “The NIST Cybersecurity Framework (CSF) 2.0,” National Institute of Standards and Technology, February 26, 2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>; “Artificial Intelligence Risk Management Framework (AI RMF 1.0),” National Institute of Standards and Technology, January 2023, <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

Free Speech

President Trump’s E.O. 14179 emphasizes the need for AI systems to be “free from ideological bias or engineered social agendas.”¹⁰ With this in mind, the AI Action Plan should emphasize First Amendment protections for free expression online and in the development of AI systems. Doing so will encourage innovation and maintain the vitality and free flow of information essential to our democracy.

The “right to compute” is a legislative concept that protects individuals’ ability to privately own and use computational technologies, such as AI and data centers, as a fundamental exercise of free speech and property rights.¹¹ Currently, bills have been proposed in states such as Montana and New Hampshire that would protect this right to compute.¹² This principle is inherently pro-free speech because computational tools are essential for modern communication, creativity, and information-sharing. By safeguarding access to these technologies, the right to compute ensures that individuals can fully exercise their First Amendment rights in a digital age. It also intersects with property rights, emphasizing autonomy over privately owned computational resources, which supports innovation and economic growth.

To advance the right to compute, the AI Action Plan should encourage federal protections for computational technologies as essential tools for free expression and innovation. The Action Plan should also encourage streamlined regulatory processes for infrastructure development, ensuring timely construction of critical infrastructure while maintaining necessary safeguards. Integrating digital rights into broader policy discussions will bolster public trust in emerging technologies while safeguarding individual freedoms. By taking these steps, the U.S. can maintain its leadership in AI innovation while protecting constitutional freedoms in an increasingly digital world.

Another recent development in AI and First Amendment rights is the creation and sharing of political deepfakes. Deepfakes are AI-generated videos or sounds that convincingly depict real people or events.¹³ Using advanced generative AI techniques, they analyze and synthesize vast amounts of visual and audio data to create highly realistic replicas. There is concern that the potential misuse of deepfakes poses significant risks, such as undermining trust in media, spreading misinformation, and influencing public opinion—especially during politically charged events like elections. As policymakers grapple with the implications of deepfake technology,

¹⁰ Exec. Order 14179.

¹¹ Right to Compute, <https://righttocompute.ai/> (last visited March 13, 2025).

¹² Montana Senate Bill 212 (2025).

¹³ “Synthetic Media & Deepfakes” Center for News, Technology & Innovation, October 11, 2024. <https://innovating.news/article/synthetic-media-deepfakes/>.

particularly in politics, they face a delicate balance between protecting against malicious uses and safeguarding free speech rights.¹⁴ Political deepfakes are simply a new form of expressing one's opinions, parody, or satire. Rather than rushing to implement broad regulatory frameworks that could inadvertently stifle free expression or innovation in AI technology, lawmakers should focus on leveraging existing laws—such as those addressing campaign impersonation, slander, and libel—to address these issues.

Section 230 of the Communications Decency Act has played a crucial role in safeguarding free speech online since the early days of the internet, and it should be left untouched in order to protect online expression as AI continues to develop. Section 230 provides immunity to interactive computer services, like social media sites, for content posted by their users.¹⁵ This protection allows platforms to host diverse user-generated content without fear of legal repercussions, fostering a vibrant ecosystem of online expression. By shielding platforms from liability for both hosting and moderating third-party content, Section 230 enables the flourishing of social media, discussion forums, and other online spaces where users can freely exchange ideas, criticize policies, and share information. If Section 230 were weakened or repealed entirely, many platforms might severely restrict user content or stop hosting it altogether, significantly limiting the internet's role as a forum for free expression and diverse viewpoints. If this were to happen, the United States risks losing a prominent avenue for free expression.

Conclusion

We are only at the beginning of the AI revolution, and the many possibilities it suggests spark excitement and ingenuity, as well as understandable concerns. America's free markets and free society enable those exciting possibilities to be realized, but many incorrectly assume that these freedoms lead to greater dangers. In reality, these same freedoms are what protect us against the risks of new technology, as we learn more about risks and adjust along with what we learn.

Former President Biden's E.O. 14148 projected today's knowledge onto tomorrow's highly uncertain AI landscape, attempting to reduce or eliminate risks. Had we continued on this path, we would have given up many of the benefits of AI, and still been unprepared to address the real risks as they became clear. By shifting the focus from "AI safety" to "AI opportunity," in the words of Vice President Vance, this Administration makes it possible to achieve both goals.

¹⁴ Richard Sill, "New York's proposed political deepfake ban suppresses speech and violates the First Amendment," Reason Foundation, February 26, 2025, <https://reason.org/commentary/new-yorks-proposed-political-deepfake-ban-suppresses-speech-and-violates-the-first-amendment/>.

¹⁵ Valerie C. Brannon and Eric N. Holmes, "Section 230: An Overview," Congressional Research Service, January 4, 2024, <https://www.congress.gov/crs-product/R46751>.

Respectfully submitted,

Max Gulker
Senior Policy Analyst, Reason Foundation
max.gulker@reason.org

Adrian Moore
Vice President of Policy, Reason Foundation

Richard Sill
Technology Policy Fellow, Reason Foundation