CED
COMMITTEE FOR ECONOMIC DEVELOPMENT
THE PUBLIC POLICY CENTER OF
THE CONFERENCE BOARD

Policy Brief: Initiatives for Federal AI Framework

May 5, 2023

Insights for What's Ahead:

Two significant developments on artificial intelligence (AI) have recently been announced by the Biden Administration. On May 4, the White House announced a new initiative to promote responsible AI innovation in an effort to protect the rights and safety of users. The initiative directly follows the Commerce Department's April 11, 2023 request which opened a 60-day comment period inviting suggestions for specific policy recommendations that would support the safe, transparent development of "trustworthy" AI for use by businesses and consumers.

- The White House initiative includes funding for seven new AI research centers and promises a proposal from OMB on policy guidance for federal use of AI systems.
- The Commerce Department is separately requesting comment on methods for regulatory assessment of AI models and sector-specific approaches.
- Federal officials are seeking participation of the private sector, including leading AI firms, to help develop supervisory frameworks around AI development and usage.
- While the federal government's efforts to develop policies that support the responsible development of AI are welcomed and commendable, the challenge is a significant one given the pace of technological advances, the many unknowns by creators themselves on how generative AI algorithms work, and the rapid release and uptake by the public of these technologies before guardrails have been placed around them.

White House AI Initiative; Public Comment Requests

On May 4, the White House announced a new initiative promoting the responsible development of AI systems. The initiative calls for the launch of seven new National AI Research Institutes under the National Science Foundation with $140 million in dedicated funding, aiming to catalyze collaborative efforts across academia, federal agencies, and industry to drive AI breakthroughs in critical areas. The announcement also stated that leading AI developers, including Microsoft, OpenAI, and Google, had committed to participate in a public evaluation of AI systems, allowing the AI models to be "evaluated by thousands of community partners and AI experts" for alignment to principles outlined in the Administration's Blueprint for an AI Bill of Rights released last October and the recent AI Risk Management Framework published by the National Institute of Standards and Technology (NIST) in January. It also announced that the Office of Management and Budget (OMB) will be releasing draft policy guidance this summer for public comment on how federal departments and agencies should use AI systems.

This announcement follows the Commerce Department's request which opened a 60-day comment period inviting suggestions for specific policy recommendations that would support the safe, transparent development of "trustworthy" AI for use by businesses and consumers. The request from the National Telecommunications and Information Administration (NTIA) specifically seeks comments on the kinds of AI audits that should be conducted, what kinds of data access would be necessary to complete the assessments, how regulators might incentivize the development of those systems, and whether different

approaches might need to apply to different industry sectors such as health care and employment. Public comments, **due by June 12**, will inform the Administration's ongoing work developing a "cohesive and comprehensive federal government approach to AI-related risks and opportunities [.]"

A group of concerns outlined in the request centers around privacy and bias of algorithmic systems, including risks introduced by AI capabilities installed into systems of facial recognition and monitoring. The White House Office of Science and Technology Policy (OSTP) on May 1 separately released its own request for information regarding employers' use of automated systems to monitor and evaluate their employees. These concerns have been central to the Administration's stance on AI risks. Vice President Harris following Thursday's meeting with tech executives released a statement that claimed, "AI has the potential to dramatically increase threats to safety and security, infringe civil rights and privacy, and erode public trust and faith in democracy." The AI Bill of Rights provided examples of those feared outcomes, including further election interference and disinformation, reproduction of bias in hiring decisions, data collection that undermines privacy, and unsafe AI implementation in areas like patient diagnosis.

AI's Rapid Advancement

The announcements follow the President's comments in early April that technology companies should ensure that their products are safe before releasing them to the public. In a meeting with science and technology advisors, the President said that "AI can help deal with some very difficult challenges like disease and climate change, but it also has to address the potential risks to our society, to our economy, to our national security."

These actions come as concerns have mounted over the rapid consumer adoption of AI tools, led by OpenAI's ChatGPT, which achieved the milestone of 100 million users faster than any technology platform in history. The pace of innovation has prompted calls from prominent figures, including Elon Musk, to pause AI experiments for six months to allow policymakers to accelerate efforts to develop safety protocols for AI design and development. Similarly, Geoffrey Hinton, who has been called "the Godfather of AI" for laying the foundation for the neural network technology powering today's AI chatbots, left Google to begin speaking freely of the dangers posed by AI. However, that push has been met with skepticism over its feasibility, "there's a lot of conversation about, 'Let's pull the plug,' but I'm not sure there is a single plug," said Arati Prabhakar, director of the White House Office of Science and Technology Policy.

A significant challenge with AI systems is the ability to explain how they arrive at their outputs. "A lot of knowledgeable people feel that explainability would help us a huge amount in promoting responsibility if we could achieve it," said Alan Davidson, Administrator of NTIA. "It is really an open question about whether we will be able to do that." That challenge has prompted the Administration to push for collaboration with the private sector, including through the recent requests for comment, on how systems can be developed to promote transparency and dependability.

Perhaps a larger concern is the ways bad actors will leverage AI technologies and how those risks can be mitigated. In Meta's quarterly threat report released this week, the company announced it had detected a rising number of malware campaigns directed at ChatGPT and similar tools. These generative AI tools also have been cited as expanding the ability to produce ever-more sophisticated malware, including by individuals without the ability to code programs.

Policymakers Consider AI Frameworks

The Administration's initiative and requests for information signal a continuation of the effort to establish a federal strategy around emerging technologies. Last October, the Administration released its Blueprint for

an AI Bill of Rights, which outlined a non-binding roadmap for the development of AI to protect privacy and avoid consumer harm, while promoting more meaningful oversight of the technology. In January, NIST also released an AI Risk Management Framework, providing a voluntary process for managing a wide range of potential AI risks. The framework proposed for AI also mirrors the direction of the Administration's National Cybersecurity Strategy released in March that similarly focuses on accountability for the largest technology platforms and service providers.

Despite those developments, no consensus has yet emerged over what methods regulators should use to oversee AI technologies or which agency should take the lead. Some in Congress have called for the creation of a new government agency to oversee AI, including Rep. Ted Lieu (D-CA), a member of the House Judiciary Committee subcommittee with jurisdiction over the internet, who said "we can harness and regulate AI to create a more utopian society or risk having an unchecked, unregulated AI push us toward a more dystopian future." Reports have also suggested that lawmakers and tech executives have discussed whether NIST could coordinate AI efforts across government.

Federal officials across agencies are beginning to review AI applications. In a joint statement in April, the FTC, CFPB, Equal Employment Opportunity Commission, and DOJ's Civil Rights Division underscored their collective commitment to leverage existing legal authorities to protect American consumers from AI-related harm. Those agencies will increasingly look towards private sector AI activities, highlighted by an FTC blog post from February warning companies that the agency was monitoring deceptive claims about AI-powered technology.

Other AI-related legislation has focused more specifically on data protection. The bipartisan American Data Privacy and Protection Act stalled last Congress and not been reintroduced. That bill would have set out a framework of rules for AI, including risk assessment obligations applying to companies developing and utilizing AI technologies, similar to those the Administration is seeking comment on. Increasing the urgency of federal officials, state and local governments have begun moving to pass their own AI-related laws—largely focused on data privacy—in the absence of comprehensive federal legislation, creating the risk of a patchwork of regulation.

AI Frameworks Progressing Globally

Governments around the world are increasingly recognizing that governance tools must be developed to mitigate the risks of autonomous systems. In the EU, the Digital Services Act adopted in November requires system audits from its large online platforms and greater transparency, while the draft Artificial Intelligence Act, approved by the European Council in December and expected to receive a positive vote in a committee of the European Parliament next week, would require "conformity assessments" of certain high-risk AI tools before deployment, with fines for noncompliance up to €30 million and would also regulate other forms of AI, including what the Act terms "general purpose" AI systems. The US and EU also signed an agreement in January to collaborate on "responsible advancements" in AI.

Italy in March became the first Western country to ban ChatGPT, ordering OpenAI to cease processing Italian users' data while a probe proceeds into the potential breach of Europe's privacy regulations. The UK also in March announced its own approach to AI regulation, calling upon regulators to develop "tailored, context-specific approaches that suit the way AI is actually being used in their sectors." Instead of establishing new regulations, the UK has pressed regulators to ensure that AI uses comply with existing laws, while also suggesting that over the next year regulators should issue additional guidance as well as other tools like risk assessment templates.

In the background of discussions on how and to what extent that AI platforms should be regulated in the US is how those frameworks might hamper the increasingly competitive race with China. However, China was one of the first movers in AI regulation, implementing requirements in March 2022 that tech

companies inform users if algorithms are being used to select content and allowing users to opt out. China has also sharply restricted consumer access to ChatGPT and other Western AI platforms, which are not officially available in the country. Recently in April, the Cyberspace Administration of China laid out draft measures to restrict the type of content that Chinese generative AI services could produce.

Conclusion

The White House initiative and recent information requests continue the momentum of federal officials to develop frameworks for regulators to assess the development of AI and risks in its use, including in the areas of data privacy and accountability. The Administration has increasingly shown efforts to collaborate and seek feedback with leading AI platforms and other private sector firms to establish the appropriate role for federal entities with regard to these emerging technologies. Public comments in response to the current and future requests will play a significant role in the Administration's eventual proposal for a comprehensive federal approach to AI-related risks and opportunities—significant challenge given the pace of technological advances, the many unknowns by creators themselves on how generative AI algorithms work, and the rapid release and uptake by the public of these technologies before guardrails have been placed around them.

About the Authors

Dr. Lori Esposito Murray is President at the Committee for Economic Development, the public policy center of The Conference Board.

Mitchell Barnes is a Senior Economic Policy Analyst at the Committee for Economic Development, the public policy center of The Conference Board.