ML STRATEGIES

The White House's Voluntary Framework for Ensuring Safe, Secure, and Trustworthy AI — AI: The Washington Report

July 27, 2023 | | By **Bruce Sokler**, **Alexander Hecht**, **Christian Tamotsu Fjeld**, Raj Gambhir

VIEWPOINT TOPICS

- Artificial Intelligence

Welcome to this week's issue of *AI: The Washington Report*, a joint undertaking of Mintz and its government affairs affiliate, ML Strategies. The accelerating advances in artificial intelligence ("AI") and the practical, legal, and policy issues AI creates have exponentially increased the federal government's interest in AI and its implications. In these weekly reports, we hope to keep our clients and friends abreast of that Washington-focused set of potential legislative, executive, and regulatory activities.

In this issue, we discuss the White House's **July 21, 2023 announcement** of a voluntary framework for ensuring safe, secure, and trustworthy AI ("July 21 Framework"). Our key takeaways are:

1. Leaders of seven major technology companies, including Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI, met with President Biden to affirm their commitment to the July 21 Framework.
2. The July 21 Framework consists of eight concrete commitments, each falling under one of three guiding principles: safety, security, and trust.
3. The announcement of this framework reaffirms the key role of the executive branch in guiding the development of comprehensive AI regulation. The Biden administration intends to issue an executive order on AI in the near future.

The White House's Voluntary Framework for "Ensuring Safe, Secure, and Trustworthy AI"

On July 21, 2023, President Biden met with the leaders of seven major technology companies to secure their commitment to a voluntary framework for responsible AI innovation. "These commitments are real," **asserted Biden**, "and they're concrete." The pronouncement of this framework ("July 21 Framework"), along with the announcement of a **forthcoming executive order** on AI, signals the resolve of the White House to maintain the strong role that the executive branch has played in guiding the development of American AI regulation. Absent substantive AI legislation from Congress, the frameworks and initiatives on autonomous systems released by the executive branch are, and will continue to be, the most concrete guidance from the federal government to businesses on AI development.

Companies representing the cutting edge of AI development, including Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI, agreed to the adoption of the July 21 Framework for AI risk management. Through these commitments, the **White House aims** to "make the most of AI's potential" by "encouraging this industry to uphold the highest standards to ensure that innovation doesn't come at the expense of Americans' rights and safety." This strategy of seeking to establish guardrails to encourage the development of AI within circumscribed boundaries is consistent with **executive branch actions going back to the Obama administration**, as well as more **nascent efforts being discussed in Congress**.

The **voluntary framework** consists of eight commitments, each falling under one of three guiding principles: safety, security, and trust.

Safety

1. Rigorously test major AI models to ensure that they are resilient, do not promote bias, and do not pose an existential risk to society.**[1]**
2. Promote the establishment of and participate in a forum or information-sharing mechanism through which companies can "develop, advance, and adopt shared standards and best practices for frontier AI safety."**[2]**

Security

3. Designate unreleased **model weights**, or parameters that AI models use to make decisions, as core intellectual property protected by cybersecurity and insider threat detection systems.
4. Establish systems that incentivize third parties to discover and report vulnerabilities in AI systems.

Trust

5. Commit to labeling AI-generated content, except content that is "readily distinguishable from reality or that is designed to be readily recognizable as generated by a company's AI system."
6. Report the capabilities, limitations, and risks of AI models to users.
7. Support research on countering the risks posed by AI systems.
8. Develop cutting-edge AI systems to help address major social issues, such as climate change and cancer detection.

Context of and Reaction to the July 21 Framework

As discussed in the **inaugural issue of this newsletter**, since the closing months of the Obama administration, regulatory efforts on AI in the United States have largely been the prerogative of the executive branch.

However, the past few months have seen Congress wade into the question of AI regulation, with members in the House and Senate releasing **targeted regulatory proposals** and **bills that would establish study groups on AI regulation**. Senate Majority Leader Chuck Schumer's (D-NY) **SAFE Innovation in the AI Age** and Representative Ted Lieu's (D-CA-36) **National AI Commission Act** each promise to lay the groundwork for robust, comprehensive AI legislation. In spite of this flurry of legislative activity, even the most **optimistic estimates** place the passage of comprehensive legislation to regulate AI at next year, if not the next session of Congress.

Given the rapid pace of technological development, and the level of **alarm expressed by experts** at the potential of AI to disrupt the economy, perpetuate bias, and promote societal risk, business leaders have been expressing the **need for immediate guidance on AI development**. Absent comprehensive legislation to regulate AI from Congress, business leaders have turned to executive branch efforts on AI. On July 19, top AI firms and research institutions published an **open letter** to Congressional leadership urging the funding of the National AI Research Resource ("NAIRR"), arguing that the body "would transform the U.S. research ecosystem and facilitate the partnerships needed to address societal-level problems."

Within this context, the White House's July 21 Framework can be seen as an attempt to provide AI developers with concrete guidance in the absence of enacted AI regulation. In a **speech delivered following the announcement of the framework**, President Biden asserted that the framework's commitments are "going to help…the industry fulfill its fundamental obligation to Americans to develop safe, secure, and trustworthy technologies that benefit society and uphold our values and our shared values."

Leaders from the seven technology companies that publically committed to the July 21 Framework lauded the administration's efforts to guide AI development. **Microsoft President Brad Smith asserted** that "the voluntary commitments address the risks presented by advanced AI models and promote the adoption of specific practices…that will propel the whole ecosystem forward." **Kent Walker, President of Global Affairs of Google and Alphabet, hailed** the July 21 Framework as "a milestone in bringing the industry

together to ensure that AI helps everyone."

But despite the enthusiasm for this framework from key industry leaders, President Biden has indicated that this and other non-binding initiatives are insufficient, and must be followed up by enforceable AI legislation. "Realizing the promise of AI by managing the risk is going to require some new laws, regulations, and oversight," **said Biden**. To ease the pathway for these "new laws" on AI, the White House has **announced the future release of an executive order** "that will ensure the federal government is doing everything in its power to advance safe, secure, and trustworthy AI and manage its risks to individuals and society."

Conclusion: Reasserting the Executive Branch's Role in Developing AI Regulation

As the 118th Congress has rapidly produced a slate of AI proposals, experts surveying the field of AI regulation have understandably turned their attention towards the legislative branch. The announcement of the July 21 Framework, along with the open letter on the NAIRR, are reminders to all those interested in the development of AI regulation in the United States to pay attention to executive branch efforts as well.

As we have discussed in **previous editions of this newsletter**, the executive branch has accumulated experience in **developing AI risk-managing frameworks**, **establishing bodies to oversee AI development**, and **collaborating with industry and academia to build regulatory competency regarding autonomous systems**. Any comprehensive regulation on AI is likely to draw from the executive branch's work on AI regulation, including the **Blueprint for an AI Bill of Rights**, the **AI Risk Management Framework**, and the forthcoming **National Priorities for Artificial Intelligence**.

As the executive and legislative branches work towards the development of comprehensive AI regulation, we will continue to monitor, analyze, and issue reports.

Endnotes

[1] Specifically, this commitment entails the use of "**red-teaming**," a strategy whereby an entity designates a team to emulate the behavior of an adversary attempting to break or exploit the entity's technological systems. As the red team discovers vulnerabilities, the entity patches them, making their technological systems resilient to actual adversaries.

[2] On July 26, 2023, four of the companies that agreed to the July 21 Framework (Microsoft, Anthropic, Google, and OpenAI) **announced the launch** of such a body. The "Frontier Model Forum" is "a new industry body focused on ensuring safe and responsible development of frontier AI models."

Authors

Bruce Sokler

Bruce D. Sokler is a Mintz antitrust attorney. His antitrust experience includes litigation, class actions, government merger reviews and investigations, and cartel-related issues. Bruce focuses on the health care, communications, and retail industries, from start-ups to Fortune 100 companies.

Alexander Hecht, Executive Vice President & Director of Operations

Alexander Hecht is Executive Vice President & Director of Operations of ML Strategies, Washington, DC. He's an attorney with over a decade of senior-level experience in Congress and trade associations. Alex helps clients with regulatory and legislative issues, including health care and technology.

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Senior Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Raj Gambhir

Raj Gambhir is a Project Analyst in Washington, DC.