Simpson Thacher

Memorandum

White House Issues Landmark Executive Order on Artificial Intelligence

November 1, 2023

On October 30, 2023, President Biden issued an extensive executive order (the "Executive Order" or the "Order") directing various Federal agencies to promulgate rules and regulations and publish best practices related to the use of artificial intelligence,[1] in an effort to "advance and govern the development and use of AI in accordance with eight guiding principles and priorities."

The Executive Order is noteworthy for several reasons. *First*, it provides a roadmap for initial rulemaking and guidance by Federal agencies related to AI. *Second*, it serves as a potential preview of future substantive laws governing the use of AI that may be enacted by Congress or state legislatures. And *third*, it represents the Executive Branch's preliminary attempt to mold the use (and potential misuse) of a nascent and fast-developing technology into existing regulatory frameworks.

Key Takeaways: Directions to Federal Agencies

The Executive Order contains numerous and far ranging directives to various Federal agencies and other executive officials, typically requiring the agency to propose regulations or issue guidelines within 90 to 270 days. Further developments from individual agencies, therefore, will be forthcoming in accordance with those schedules. Some of the most significant directives issued by the Executive Order include:

- directing the Department of Commerce, through the authority of the Defense Productive Act, to require companies developing advanced AI models to share safety test results and other data with the Federal government;

- directing the Treasury Department to "issue a report on best practices for financial institutions to manage AI-specific cybersecurity risks;"

- directing the Department of Health and Human Services to establish a task force to address the use of predictive and generative AI technology in healthcare delivery and financing, "including quality measurement, performance improvement, program integrity, benefits administration, and patient experience;"

---

[1] Artificial intelligence, commonly referred to as "AI," is defined in the Executive Order as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments." This definition is codified in Federal law at 15 U.S.C. § 9401(3).

- directing the Department of Labor to "develop and publish principles and best practices for employers that could be used to mitigate AI's potential harms to employees' well-being and maximize its potential benefits," including related to "implications for workers of employers' AI-related collection and use of data about them, including transparency, engagement, management, and activity protected under worker-protection laws;"

- directing the Department of Commerce to submit a report identifying current and potential future tools for detecting, identifying, and authenticating synthetic content created by AI systems; and

- directing the Department of Homeland Security to publish on a new website (AI.gov) "a clear and comprehensive guide for experts in AI and other critical and emerging technologies to understand their options for working in the United States."

The Executive Order does not apply to the independent regulatory agencies (such as the SEC, FTC, or FDIC), but it specifically "encourage[s]" the independent agencies to, among other things:

- "consider whether to mandate guidance through regulatory action in their areas of authority and responsibility" with respect to infrastructure and cybersecurity;

- "consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, including risks to financial stability;" and

- "consider rulemaking, as well as emphasizing or clarifying where existing regulations and guidance apply to AI, including clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and emphasizing or clarifying requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models."

The Executive Order establishes a preliminary framework for the Federal regulation of AI by assigning various responsibilities to different agencies. The Order sets various deadlines by which these agencies shall promulgate new AI-related rules or industry guidance, but does not expressly indicate if and how these promulgated rules will be enforced.

Based on the subject areas addressed in the Executive Order, technology developers, healthcare firms, financial institutions, and other large corporations whose employees or customers interact with AI-related processes or systems on a regular basis may be particularly implicated by the upcoming regulations and best practices issued pursuant to the Order.

Other Key Takeaways: Reporting Requirements for Training Certain AI Models and Infrastructure-as-a-Service Providers

A significant section of the Executive Order sets new reporting requirements for companies training sophisticated AI models and for Infrastructure-as-a-Service ("IaaS") Providers, including both Providers based in the United

States and "foreign resellers of United States IaaS products." For example, Section 4.2(b) of the Executive Order directs the Department of Commerce to require "Companies developing or demonstrating an intent to develop potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records" regarding various subjects, including but not limited to the training or development of such models, and physical and cybersecurity measures taken to protect the models. Pending the issuance of more detailed regulations by the Commerce Department, the Executive Order defines "dual-use foundation models" broadly to include (1) "any model that was trained using a quantity of computing power greater than 10^{26} integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 10^{23} integer or floating-point operations;" or (2) "any computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum computing capacity of 10^{20} integer or floating-point operations per second for training AI."

Section 4.2(c) of the Order directs the Department of Commerce to propose regulations that require United States IaaS Providers "to submit a report to the Secretary of Commerce when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. These reports will include "at a minimum, the identity of the foreign person and the existence of any training run of an AI model meeting the criteria set forth" in the Executive Order as amended by future regulations. Although the regulatory landscape may evolve with future regulatory action, it appears that a foreign company providing cloud computing services with its servers in a foreign country using United States chips will not be considered a "United States IaaS Provider" or a "foreign reseller of United States IaaS products," for the purposes of the Executive Order, and therefore is unlikely to be subject to the reporting requirements provided by Section 4.2(c) at present.

Further guidance to firms training advanced AI models that fall under the requirements of these sections will be available once the Department of Commerce issues its proposed regulations.

Potential Future Legislative Action

Although various states have enacted laws implicating earlier uses of AI (such as in the context of data privacy), neither Congress nor any state legislature has yet enacted laws related to the generative or predictive AI software with which people have become familiar in 2023. Initial legislative attempts to regulate this new technology remain in their infancy. For example, in September 2023, a bill was introduced in California—home to many of the most significant industry players—that seeks to establish a "safety framework" for AI, including setting transparency requirements for AI systems that exceed certain quantities of computing requirements, and implementing security measures to protect proprietary AI models from theft.

The Executive Order may hasten efforts by states who have thus far been adopting a wait-and-see approach for the regulation of AI, given the interest of certain states—such as California—in pioneering legislation governing the use of new technologies. Although a robust legal framework for AI formally established by Congress or state

legislatures may still be several years away, the Executive Order marks a key first step in how government actors will attempt to promote safeguards—whether in the context of privacy, industry abuse, consumer protection, or national security—around an emerging technology that presents both significant benefits and challenges.

* * *

The authors of this memo at Simpson Thacher are continuing to monitor developments in this field, and welcome any questions related to this Executive Order, or any other legal or regulatory implications of AI.

For further information regarding this memorandum, please contact one of the following authors:

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

George S. Wang
+1-212-455-2228
gwang@stblaw.com

Daniel S. Levien
+1-212-455-7092
daniel.levien@stblaw.com

Andrew W. Marrero
+1-212-455-2450
andrew.marrero@stblaw.com

WASHINGTON, D.C.

Abram J. Ellis
+1-202-636-5579
aellis@stblaw.com

BEIJING

Shuhao Fan
+86-10-5965-2987
shuhao.fan@stblaw.com