ML STRATEGIES

Federal Agencies Continue to Take Action on AI Pursuant to AI EO — AI: The Washington Report

July 11, 2024 | | By **Bruce Sokler**, **Alexander Hecht**, **Christian Tamotsu Fjeld**, Matthew Tikhonovsky

VIEWPOINT TOPICS

- Artificial Intelligence

1. President Biden's October 2023 **Executive Order on AI** directed various agencies to take certain actions by June 26, 2024 — 240 days after the EO's issuance.
2. The 240-day actions involved steps by agencies to strengthen data privacy, identify techniques for labeling and authenticating AI-generated content, and curb the dissemination of AI-generated explicit content.
3. Specifically, on June 26, 2024, the National Science Foundation (NSF) launched a program to fund projects that enhance data privacy.
4. The National Institute of Technology (NIST) issued a draft report on techniques for labeling and authenticating AI-generated content and limiting AI-generated explicit content.

President Joe Biden's October 2023 **Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence** (AI EO) directed various federal agencies to take certain actions related to AI. As we covered in the **AI EO timeline**, June 26, 2024 — the 240-day mark after the EO's issuance — was the deadline for agency actions to strengthen data privacy and label and authenticate AI-generated content. In this newsletter, we cover the two main actions that were taken 240 days after the signing of the EO.

NSF Launches Funding Program for Privacy-Enhancing Technologies

As AI technologies have evolved and proliferated in recent years, concerns about data privacy have been top of mind for various regulators and policymakers. In March 2023, the National Science and Technology Council (NSTC) published its "***National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (PPDSA)***." According to the strategy document, PPDSAs are "methodological, technical, and sociotechnical approaches that employ privacy-enhancing technologies to derive value from, and enable an analysis of, data to drive innovation while also providing privacy and security." NSTC's strategy creates a framework for mitigating the privacy-related risks associated with technologies used for data analysis, including artificial intelligence.

In October 2023, Biden's AI EO also underscored the need for protecting data privacy. The EO tasked the NSF to, within 240 days of the EO, "engage with agencies to identify ongoing work and potential opportunities to incorporate [privacy-enhancing technologies (PETs)] into their operations." PETs include a broad range of tools aimed at protecting privacy, including differential privacy and end-to-end encryption. The EO also directed the NSF to "where feasible and appropriate prioritize research — including efforts to translate research discoveries into practical applications — that encourage the adoption of leading-edge PET solutions for agencies' use, including through research engagement."

Building off the NSTC strategy document and pursuant to the AI EO, on June 26, 2024, the **NSF launched** the **Privacy-Preserving Data Sharing in Practice (PDaSP)** program. The program seeks solicitations for three main tracks of project funding:

- **Track 1: "Advancing key technologies to enable practical PPDSA solutions"** – This track focuses on maturing PPDSA technologies and combinations of such technologies, with an emphasis on "transitioning theory to practice for the key PPDSA technique(s) considered."
- **Track 2: "Integrated and comprehensive solutions for trustworthy data sharing in application settings"** – This track supports integrated privacy management solutions, with a focus on solutions for different use-cases and application contexts, including various technological, legal, and regulatory contexts.

- **Track 3: "Usable tools and testbeds for trustworthy sharing of private or otherwise confidential data"** – This track emphasizes the need "to develop tools and testbeds to support and accelerate the adoption of PPDSA technologies." Currently, stakeholders face various barriers to adopting such technologies, including "due to a lack of effective and easy-to-use tools," that this track seeks to overcome.

The PDaSP program is supported by partnerships with other federal agencies and industry. Current funding partners include Intel Corporation, VMware LLC, the Federal Highway Administration, the Department of Transportation, and the Department of Commerce. The NSF is also open to collaborating with other agencies and organizations that are interested in co-funding projects. Project funding is expected to range from $500,000 to $1.5 million for up to three years.

NIST Issues Draft Guidance on Synthetic Content

Policymakers have also been focused on concerns related to synthetic content — audio, visual, or textual information that has been generated or significantly altered by AI. The AI EO specifically directed the Secretary of Commerce along with other relevant agencies to identify, within 240 days after the EO, the "existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for" authenticating content, labeling synthetic content, and "preventing generative AI from producing child sexual abuse material or producing non-consensual intimate images of real individuals."

On April 29, 2024, pursuant to the AI EO, the Department of Commerce's National Institute of Technology (NIST) published a draft report on "***Reducing Risks Posed by Synthetic Content***." The draft report covers three main topic areas, as discussed below.

First, the report covers two data tracking techniques for disclosing that content is generated or modified by AI: digital watermarking and metadata recording. While digital watermarking "involves embedding information into content (image, text, audio, video)" to indicate that the content is synthetic, metadata recording stores information about the content's properties and makes it accessible, allowing an interested party to "verify the origins of content and how the history of content may [have changed] over time," according to the report.

Second, the report outlines best practices for testing and evaluating data tracking and synthetic content detection technologies, including techniques for testing digital watermarking and metadata recording techniques and automated content-based detection techniques.

Finally, the report overviews specific techniques for preventing harm from Child Sexual Abuse Material (CSAM) and Non-Consensual Intimate Imagery (NCII) that are created or disseminated by AI. The report discusses techniques for filtering CSAM and NCII out of data used to train AI systems, blocking the output of AI-generated images that potentially contain CSAM or NCII, and hashing confirmed synthetic CSAM and NCII to prevent its further distribution.

Comments on the draft report were submitted by June 2, 2024. While the final report was due on June 26, 2024, it has not been made publicly available.

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.

Matthew Tikhonovsky

Matthew is a Mintz Senior Project Analyst based in Washington, DC.