Proskauer

President Issues Sweeping Executive Order to Manage Risks of AI

New Media and Technology Law Blog on **October 30, 2023**

On October 30, 2023, President Biden issued an "Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence" designed to spur new AI safety and security standards, encourage the development of privacy-preserving technologies in conjunction with AI training, address certain instances of algorithmic discrimination, advance the responsible use of AI in healthcare, study the impacts of AI on the labor market, support AI research and a competitive environment in the industry, and issue guidance on the use of AI by federal agencies. This latest move builds on the White House's previously-released "Blueprint for an AI Bill of Rights" and its announcement this past summer that it had secured voluntary commitments from major AI companies focusing on what the White House termed as "three principles that must be fundamental to the future of AI – safety, security, and trust."

There is some bipartisan appetite for AI regulation in Congress, with members having introduced several bills and committees continuing to hold hearings to elucidate the issues. Yet, the passage of any AI legislation remains uncertain.[1]

The Executive Order offers some insight into the types of issues that concern the White House and regulators (particularly surrounding AI security, privacy and discrimination) and the types of standards surrounding trust and security that may emerge around AI in the coming year. AI developers have been open to common sense, light touch regulation. Indeed, OpenAI CEO Sam Altman, in his written testimony before the Senate Judiciary Committee, stated: "We believe it is essential to develop regulations that incentivize AI safety while ensuring that people are able to access the technology's many benefits." Thus, the Executive Order is expected to be an important driver for the development and deployment of AI in the U.S. and the development of related security standards going forward.

Below is an outline of the pertinent items in the Executive Order (EO):

- **New standards for safety and security**: One of the most striking aspects of the EO is that the President has invoked the Defense Production Act and will require that "developers of the most powerful AI systems share their safety test results and other critical information with the U.S. government." Specifically, the EO requires "that companies developing any foundation model that poses a serious risk to national security, national economic security, or national public health and safety must notify the federal government when training the model, and must share the results of all red-team safety tests." In addition, surrounding AI safety and trust, the EO directs the National Institute of Standards and Technology (NIST) to set "rigorous standards" for red-team testing to ensure safety before public release, which the Department of Homeland Security (DHS) will then apply to critical infrastructure sectors and thereafter establish the AI Safety and Security Board. The extent of this Board's scope and influence remains to be seen, including how such a board would work in tandem with any independent oversight body that might be established by future AI legislation (see e.g., the Blumenthal-Hawley AI legislation framework, which contemplates the establishment of a licensing regime administered by an independent oversight body). The EO further directs the Department of Commerce to develop guidance for content authentication and watermarking to clearly label AI-generated content (a requirement that is central to a new bill introduced last week by Senators Schatz and Kennedy). Lastly, the EO encourages the development of an advanced cybersecurity program to develop AI tools to shore up critical software.
- **Privacy:** The EO expresses the President's support for passage of a comprehensive data privacy law and then advances a few AI-related privacy aims, including prioritizing the development of "privacy-preserving techniques" related to the use of AI training data, developing privacy guidance for federal agencies to account for AI privacy risks, and producing guidelines for evaluating the effectiveness of privacy-preserving techniques in AI systems. [The EO directs the evaluation of how agencies collect and use commercially available data, an issue that has been the subject of Congressional hearings and data privacy advocacy group concern].
- **Anti-discrimination**: The EO focuses on algorithmic discrimination, as it directs agencies to provide anti-discrimination guidance to landlords, federal benefits programs, and federal contractors over their use of AI algorithms and also to coordinate on best practices for investigating and enforcing civil rights violations related to AI.
- **Healthcare**: The EO directs the Department of Health and Human Services (HHS) to advance the responsible use of AI in healthcare and drug development by establishing a safety program to receive reports of and remedy harms or unsafe healthcare practices involving AI.

- **Labor market**: Much like other technological developments in the last century, the further development and deployment of AI is expected to displace workers as certain tasks become more automated. The White House directed the development of principles to address job displacement and workplace equity.
- **Innovation**: The EO seeks to ensure the U.S. maintains leadership in AI, continues its participation in developing international AI standards and also broadens research opportunities for students and entrepreneurs/small businesses to promote a robust and fair AI ecosystem, as well as expand existing authorities to attract talented individuals from abroad to study and stay in the country.

---

[1] Taking a wider view, at the moment new laws that target AI developers in the EU, UK and the U.S. appear only in draft form or as non-binding guidance, or have otherwise not yet come into effect (though, EU trilogue negotiations among the EU Council, Parliament and Commission may produce a final version of the EU AI Act before the end of the year). Unlike the Executive Order, which primarily focuses on harnessing federal agency action surrounding AI standards and principles, the EU AI Act would seek to regulate a broad category of AI applications in the public and private sector under a risk-based approach to regulation, grouping AI systems into risk categories and specifying requirements for auditing, transparency and other obligations for each category.

View original.

Related Professionals

- **Jeffrey D. Neuburger**