LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

White House AI Order Balances Innovation And Regulation

By **Kristen Logan and Martin Zoltick** (November 6, 2023, 8:37 AM EST)

Kristen Logan

Martin Zoltick

On Oct. 30, President Joe Biden issued an executive order on safe, secure and trustworthy artificial intelligence.[1]

The executive order provides a sprawling list of directives aimed at establishing standards for AI safety and security and protecting privacy.

While the executive order acknowledges the executive branch's lack of authority for any lawmaking or rulemaking, AI stakeholders and their advisers, as well as companies using or planning to use AI, should consider the directives detailed in the executive order as a good indicator of where the regulatory and legislative landscape may be heading in the U.S.

At a minimum, the detailed directives will likely be considered important indicators for establishing best practices when it comes to the development and use of AI.

Broad Definition of Artificial Intelligence

The executive order adopts the definition of artificial intelligence from Title 15 of the U.S. Code, Section 9401, the statutory codification of the National AI Initiative Act of 2020.

The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to:

- Perceive real and virtual environments;
- Abstract such perceptions into models through analysis in an automated manner; and
- Use model inference to formulate options for information or action.

While much of the current headlines surrounding the use of AI and the calls for regulation concerns generative AI, or GAI, models and applications, the definition provided in the executive order is much broader than simply GAI and, essentially, applies to all types of AI, including AI that has been in popular use for many years.

Thus, despite the current focus on GAI models, companies employing any type of AI technology should be on notice that their activities might be implicated by the directives outlined in the executive order.

Specific Directives to Agencies

The executive order outlines specific directives to numerous federal agencies for examining and addressing the use of AI in certain sectors.

Many of these directives concern federal agencies in "critical" fields like health care, financial services, education, housing, law enforcement and transportation.

The executive order, while lacking the authority to create new privacy laws, urges these agencies to provide guidance with respect to how existing privacy standards and regulations apply to AI. For example, the executive order includes the following directives:

- With respect to the health and human services sector, the executive order urges the secretary of health and human services to provide guidance on the "incorporation of safety, privacy, and security standards into the software development lifecycle for protection of personally identifiable information";
- The executive order also directs the secretary of health and human services to issue guidance, or take other action, in response to noncompliance with privacy laws as they relate to AI;
- The secretary of education is required to develop an AI toolkit that includes guidance for designing AI systems to align with privacy-related laws and regulations in the educational context; and
- The executive order encourages the Federal Trade Commission to consider whether to exercise its existing authorities to ensure that consumers and workers are protected from harms that may be enabled by the use of AI.

Though the executive order urges the application of existing privacy laws to AI, the executive order also recognizes the executive branch's lack of lawmaking authority and makes a call to the U.S. Congress to pass bipartisan data privacy legislation.

The executive order also addresses GAI and, specifically, reducing the risks posed by synthetic content, defined as "information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI."

The executive order directs the secretary of commerce, in consultation with the heads of other relevant agencies, to submit a report identifying the existing standards, tools, methods and practices, as well as the potential development of further science-backed standards and techniques, for:

- Authenticating content and tracking its provenance;
- Labeling synthetic content, such as using watermarking;
- Detecting synthetic content;
- Preventing generative AI from producing child sexual abuse material or producing nonconsensual intimate imagery of real individuals — to include intimate digital depictions of the body or body parts of an identifiable individual;
- Testing software used for the above purposes; and
- Auditing and maintaining synthetic content.

Ultimately, the report will be used to issue guidance to agencies for labeling and authenticating such content that they produce or publish.

The executive order includes several directives that call for the development guidelines, standards, and best practices for AI safety and security.

The executive order instructs the secretary of commerce, acting through the director of the National Institute of Standards and Technology and in coordination with the secretary of energy and the

secretary of homeland security to

> establish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems, including developing companion resources to the AI Risk Management Framework and to the Secure Software Development Framework to incorporate secure development practices for generative AI and for dual-use foundation models, as well as launching an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity.

The executive order directs the secretary of homeland security to establish an Artificial Intelligence Safety and Security Board as an advisory committee, which will made up of AI experts from the private sector, academia and government.

This newly established board will provide to the secretary of homeland security and the federal government's critical infrastructure community advice, information, and recommendations for improving security, resilience and incident response related to AI usage in critical infrastructure.

Another important topic addressed by the executive order relates to patents and copyrights — the patentability of inventions developed using AI, including the issue of inventorship, and the scope of copyright protection for works produced using AI.

The executive order directs the undersecretary of commerce for intellectual property and the director of the U.S. Patent and Trademark Office to publish guidance to USPTO patent examiners and applicants addressing inventorship and the use of AI, including generative AI, in the inventive process, and other considerations at the intersection of AI and IP, which could include updated guidance on patent eligibility to address innovation in AI and critical and emerging technologies.

The executive order directs the U.S. Copyright Office to issue recommendations to the president on potential executive actions relating to copyright and AI.

The recommendations shall address any copyright and related issues discussed in the Copyright Office's study, including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training.

Development of Privacy-Enhancing Technologies

The executive order also supports the research and development of privacy-enhancing technologies, or PETs, that mitigate privacy risks arising from data processing.

The order defines PETs as including secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy and synthetic-data-generation tools. The executive order's support of these technologies underscores the importance of taking a privacy-by-design approach during the development lifecycle.

While the executive order cannot require private companies to adopt PETs, the executive order does require that federal agencies use PETs when appropriate. However, the fact that the executive order cannot set this requirement for private companies does not insulate these companies from liability.

For example, FTC enforcement actions often assess whether an entity adopted "reasonable" privacy and data security measures based on technology that is readily available.

Because the executive order seeks to increase the development and adoption of PETs, it is only a matter of time before agencies like the FTC consider the use of these PETs necessary for carrying out reasonable privacy and data security measures.

Regulations for Developers of Dual-Use Foundation Models

Applying the Defense Production Act, the executive order requires that developers of dual-use foundation models share safety test results with the U.S. government. The executive order defines

"dual-use foundation model" to mean:

> [A]n AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters

This definition includes models that implement technical safeguards designed to prevent users from taking advantage of the model's unsafe capabilities. For reference, existing models encompassed by this definition include OpenAI LLC's GPT4, some versions of Meta Platforms Inc.'s Llama 2 model, Anthropic PBC's Claude 2 and Google LLC's PaLM 2 model.

Given that in the AI space bigger is better, the executive order's requirement that dual-use foundation models contain at least tens of billions of parameters will likely not result in a significant carve out as GAI models continue to progress.

Thus, the executive order's regulations with respect to these models will likely apply to both incumbent companies as well as companies looking to enter the space. Additionally, it is unclear how far this definition will extend.

For example, does this definition extend to companies that further train and fine-tune a third party's foundation model? It is possible that the executive order definition of dual-use foundation model includes models fine-tuned using services like Amazon.com Inc.'s Bedrock, which allows developers to further train foundation models.

Accordingly, companies that further train a third party's foundation model should be on notice of the potential applicability of this definition.

Relying upon the Defense Production Act, the executive order requires companies developing or demonstrating an intent to develop dual-use foundation models to submit information, reports, and records regarding the training, development, and production of such models. The submissions would include the results of red-team safety tests and documentation concerning ownership and protection of the model's weights and parameters.

The executive order defines "AI red-teaming" to encompass structured testing efforts to find flaws and vulnerabilities in an AI system and provides that the secretary of commerce will establish guidelines for conducting AI red-teaming tests.

However, the executive order does not provide any guidance as to how companies can balance submitting the required documents and information while still maintaining trade secret protection, satisfying obligations of confidentiality or complying with contract provisions and legal requirements that may be applicable.

Navigating the tension between compliance and these other considerations will certainly be a primary concern for companies required to abide by these reporting requirements.

Notably, in line with the July 21 voluntary commitments from leading AI companies, the executive order reinforces the de facto standard to maintain model weights as highly confidential trade secrets.

The executive order provides that the secretary of commerce shall solicit input from the private sector, academia, civic society and other stakeholders concerning the risks and benefits of models having widely available weights.

Companies developing or seeking to develop open-source large language models will want to monitor developments on this front.

The executive order also suggests that the reporting requirements under the Defense Protection Act would additionally apply to models and computing clusters of a certain size.

Specifically, until the secretary of commerce defines different technical conditions, these reporting

requirements are deemed to additionally apply to:

> Any model that was trained using a quantity of computing power greater than 1026 integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 1023 integer or floating-point operations.
>
> Any computing cluster that has a set of machines physically co-located in a single data center, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum computing capacity of 1020 integer or floating-point operations per second for training AI.

The executive order does not constrain these additional categories of models and computing clusters to only dual-use foundation models using this amount of computing power.

Because these technical conditions are subject to change and updates on a regular basis, companies developing AI models not falling within the definition of a dual-use foundation model should be on notice of the potential applicability of these provisions.

Conclusion

The foregoing highlights just some of the many directives included in the extensive executive order.

The executive order is jam-packed with calls to establish numerous boards, institutes, task forces and groups each tasked with differing responsibilities around establishing new standards for AI safety and security, protecting Americans' privacy, advancing equity and civil rights, standing up for consumers and workers, promoting innovation and competition, and advancing American leadership around the world.

Anyone involved in the AI space would be well advised to keep a close watch on the follow through of these numerous directives.

They will, no doubt, shape the regulatory and legislative landscape in the U.S. as it evolves over the coming months and years, and may help strike the balance between the freedom to innovate in this rapidly evolving space and the need to impose some level of regulation. Much more to follow.

Kristen Logan is an associate and Martin Zoltick is a member at Rothwell Figg Ernst & Manbeck PC.

Rothwell Figg members Jenny Colgate and Jennifer Maisel contributed to this article.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
