Executive Order on Artificial Intelligence Puts Focus on Privacy and Cybersecurity Considerations for AI Development

11.09.2023

***Key Takeaways*:** The recent Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence marks a major step toward the regulation of AI development and use in the U.S. The Order establishes notification requirements for the development of large-scale AI models and directs the creation of new AI-specific cybersecurity standards. Additionally, the Order instructs several federal agencies to develop policies and frameworks for addressing the risks that AI may pose to individuals whose data is used to train AI models or who are subject to decisions made using AI tools.

On October 30, 2023, President Joe Biden issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (the "Order") intended to require greater transparency from artificial intelligence ("AI") companies and improve the safety and security of the use of AI products and services offered in the United States. While the Order takes steps toward establishing best practices and standards for AI, it is not clear how, or whether, the directives of the Order will be enforced. Nonetheless, the Order has been well received by tech companies and is largely viewed as a key step toward a comprehensive system of AI governance. Key features of the Order are discussed below.

ATTORNEYS

Maureen E. Fulton

Mikaela M. Witherspoon

PRACTICE AREAS

Artificial Intelligence

Data Privacy and Security

Executive Order on Artificial Intelligence Puts Focus on Privacy and Cybersecurity Considerations for AI Development

NIST Standards

Within 270 days of the date of the Order, the National Institute of Standards and Testing ("NIST") in coordination with the Secretary of Energy, the Secretary of Homeland Security, and the heads of other relevant agencies as appropriate, must develop guidelines and best practices for developing and launching safe, secure, and trustworthy AI systems, with the intent of promoting consensus industry standards. This includes establishing standards for "red team" testing – testing intended to break AI models in order to demonstrate vulnerabilities in the models prior to the launch of new AI models and developing a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI.

The forthcoming NIST standards will be utilized by the Department of Homeland Security to address critical infrastructure sectors and establish the AI Safety and Security Board. However, the Order does not require AI companies to follow NIST standards or testing methods.

On November 1, 2023, Vice President Kamala Harris announced a series of U.S. initiatives regarding the safe use of AI, including a new United States AI Safety Institute ("U.S. AISI") within NIST. The U.S. AISI will operationalize NIST's AI Risk Management Framework by creating new guidelines, tools, benchmarks, and best practices for evaluating and mitigating AI risk. In addition, the U.S. AISI will develop technical guidance to be used by regulators when considering rulemaking and enforcement on AI issues such as algorithmic discrimination, and will partner with experts and organizations by in the U.S. and internationally for information-sharing and research purposes.

Requirement to Notify Federal Government of High Risk AI Models

The Order establishes a requirement, effective 90 days after the date of the Order, for all U.S. companies developing new large-scale AI models that exceed a specific threshold to notify the federal government during training of the model, and to share the results of safety tests and other key information with the federal government pursuant to the Defense Production Act. The threshold is intended to capture only large-scale AI models trained on extensive amounts of data, such as Open AI's ChatGPT, that could pose risks to national security, national economic security, or national public health and safety due to the large quantities of data consumed for training. A White House spokesperson indicated that this requirement will apply to future commercial AI models in the U.S., but will likely not be enforced for AI models that were launched prior to the Order.

Executive Order on Artificial Intelligence Puts Focus on Privacy and Cybersecurity Considerations for AI Development

The Order also takes steps to address the risk of foreign malicious cyber actors, directing the Secretary of Commerce, within 90 days of the date of the Order, to propose regulations requiring U.S. providers of infrastructure as a service ("IaaS") products to submit a report to the Secretary of Commerce when a foreign person transacts with the provider to train a large AI model with potential capabilities to be used in malicious cyber activity. Such reports must include the identity of the foreign person and the existence of any training activity of an AI model meeting specific computing power criteria, as well as any additional information identified by the Secretary.

Federal Agency Guidance and Tasks

The Order requires federal agencies to create rules and guidelines for various uses of AI in order to protect against bias in the application of AI products, ensure consumer privacy, and manage cybersecurity risks. This includes directives in the following areas:

- National Security: The Department of Energy and the Department of Homeland Security will work together to address the risk of AI systems to critical infrastructure, as well as potential chemical, biological, radiological, nuclear, and cybersecurity threats. The Department of Homeland Security will establish an Artificial Intelligence Safety and Security Board as an advisory committee intended to provide advice, information, or recommendations for improving security, resilience, and incident response related to AI usage in critical infrastructure. The National Security Council will also be required to develop a memorandum on how the intelligence and military communities utilize AI and how to best counteract the actions of adversaries regarding AI technologies.
- Health and Human Services: The Secretary of Health and Human Services, along with the Secretary of Defense and Secretary of Veterans Affairs are to develop a Health and Human Services AI Task Force. The AI Task Force will develop a strategic plan that includes policies and frameworks, including regulatory action, as appropriate, on the responsible deployment and use of AI in the health and human services sector (including research and discovery, drug and device safety, healthcare delivery and financing, and public health). Further, the Secretary of Health and Human Services is directed to consider the development of guidance or other actions against healthcare providers regarding noncompliance with federal privacy laws related to AI.
- Education: The Secretary of Education is directed to develop resources regarding nondiscriminatory uses of AI in the education context, including the impact AI systems have on vulnerable and underserved communities. This will include the development of an "AI toolkit" for educators that includes recommendations from the Department of Education's AI and the Future of Teaching and Learning report, including appropriate human review of AI

Executive Order on Artificial Intelligence Puts Focus on Privacy and Cybersecurity Considerations for AI Development

decisions, designing AI systems to enhance trust and safety and align with privacy-related laws and regulations in the educational context, and developing education-specific guardrails.

- Discrimination and Civil Rights: Relevant federal agencies will be required to issue guidance on how landlords, federal benefit programs, and contractors can use AI in an effort to reduce discrimination and bias that can occur when using AI. The Department of Justice will be required to train civil rights offices on best practices for prosecuting civil rights violations related to AI, and to establish standards for the use of AI in the criminal justice system.

Privacy Protections

The Order acknowledges that the use of AI comes with risks to personal information and data privacy, as AI makes it easier to extract, identify, and exploit personal data, and heightens incentives to do as companies use data to train their AI systems. In an effort to combat the risk of exploitation of personal data in AI models as well as the potential exposure of sensitive data, the federal government will take action to ensure that the collection, use, and retention of data is lawful and secure, and mitigates confidentiality and privacy risks.

Further, federal agencies are directed to use available policy and technical tools to protect against the risk of improper collection and use of personal data. This includes a requirement for federal agencies to study the effect of current data privacy protections and develop new techniques as necessary. Federal agencies will be required to study how they collect and utilize personal information, including personal information purchased from data brokers. The Order also directs the National Science Foundation to develop stronger cryptography protections aimed at protecting privacy and national security as the field of AI continues to develop.

Within 120 days of the date of the Order, the Director of the National Science Foundation, together with the Secretary of Energy, must fund the creation of a Research Coordination Network aimed at advancing privacy research, including the development, deployment, and scaling of privacy-enhancing technologies ("PETs"). The Research Coordination Network will allow privacy researchers to share information, collaborate on research, and develop standards for the privacy research community.

The Order also calls on Congress to pass comprehensive privacy legislation that would address the potential privacy risks posed by AI. There is increasing discussion of potential AI legislation, with Senate Majority Leader Chuck Schumer urging Congress to act on the regulation of AI in his response to the Order.

Executive Order on Artificial Intelligence Puts Focus on Privacy and Cybersecurity Considerations for AI Development

Koley Jessen will continue to monitor developments related to AI regulation in the U.S. and advise as updates become available. If you have questions as to how to best utilize AI in accordance with data privacy laws, please contact one of the specialists in our **Data Privacy and Security** or **Artificial Intelligence** practice areas.