AN A.S. PRATT PUBLICATION
FEBRUARY 2024
VOL. 10 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 2** **February 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

President Biden's Executive Order Enables Agencies to Address Key Artificial Intelligence Risks

By Michael La Marca, Lisa Sotto and Liliana Fiorenti*

In this article, the authors set forth key takeaways from President Biden's recent executive order on artificial intelligence.

On October 30, 2023, President Joe Biden signed a sweeping executive order on safeguards relating to artificial intelligence (AI).[1] The Executive Order (EO) on Safe, Secure, and Trustworthy Artificial Intelligence is designed to promote a coordinated approach across the federal government for the safe and responsible development and use of AI. The EO also builds upon prior steps the Biden Administration has taken to address responsible AI innovation, including its (1) October 2022 Blueprint for an AI Bill of Rights,[2] a nonbinding set of guidelines for the design, development and deployment of AI systems, and (2) July 2023 announcement that it had secured voluntary commitments from several leading AI companies regarding the management of AI risks in a safe, secure and trustworthy manner.[3]

The EO is applicable to the federal government, although its requirements will indirectly affect both developers and downstream users of AI systems.[4] Most notably, the EO invokes the Defense Production Act[5] to direct the Secretary of Commerce to implement federal government reporting requirements for companies developing certain "foundational" AI models that pose a serious risk to national security, national economic security or national public health and safety.

---

* Michael La Marca (mlamarca@huntonak.com), a partner in the New York office of Hunton Andrews Kurth, advises companies on cutting-edge technologies and information practices. Lisa Sotto (lsotto@huntonak.com) is a partner in the firm's New York office and chair of the firm's Global Privacy and Cybersecurity practice group. Liliana Fiorenti is a law clerk in the firm's New York office.

[1] Executive Order on Safe, Secure and Trustworthy Artificial Intelligence (AI) (2023), EO 14110, 88 Fed. Reg. 75191-75226, 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/.

[2] Blueprint for an AI Bill of Rights: Making Automated Systems Work For The American People (October 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[3] Remarks by President Biden on Artificial Intelligence (July 21, 2023), https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/07/21/remarks-by-president-biden-on-artificial-intelligence/.

[4] The EO defines "AI" 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. 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.

[5] 50 U.S.C. 4501 et seq.

More generally, the EO directs or encourages various federal government agencies to take a series of actions across the following eight domains:

- Safety and security;
- Privacy;
- Equity and civil rights;
- Protections for consumers, patients and students;
- Protections for workers;
- Intellectual property;
- Innovation and competition; and
- Responsible and effective government use of AI.

Because most of the EO's requirements rely on actions from various federal government agencies as directed by the EO, they do not have an immediate effect on the AI marketplace. That said, absent comprehensive federal AI legislation, the EO serves as a de facto roadmap for AI regulatory priorities moving forward.

KEY TAKEAWAYS FROM THE EO ON AI

Key takeaways from the EO on AI include:

AI Safety and Security

Reporting Requirements

Within 90 days of the EO, the Secretary of Commerce, in consultation with other federal government agencies, must adopt reporting requirements for companies developing or demonstrating an intent to develop certain higher risk foundational models referred to as "dual-use foundation models." "Dual-use foundation models" generally refers to those AI models that:

(1) Are trained on broad data;

(2) Generally use self-supervision;

(3) Contain at least tens of billions of parameters;

(4) Are applicable across a wide range of contexts; and

(5) Exhibit, 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 and/or safety.

Such companies will be required to report to the federal government, on an ongoing basis, activities related to training, developing or producing the models, information relating to the relevant model itself, and the results of relevant "red team" safety testing (as described below) along with descriptions of associated measures taken to strengthen model security and address weaknesses identified during testing.

Red-Team Requirements

Within 270 days of the EO, the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), and in consultation with other federal agencies, must also establish guidelines to enable developers of AI, particularly developers of dual-use foundation models, to conduct AI "red-teaming tests" which use adversarial methods to find flaws or vulnerabilities in an AI system, "such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system."

New Standards and Guidance

The EO calls for the establishment of new AI-related standards and federal guidance for the development and deployment of safe, secure and trustworthy AI systems. For example, in addition to the development of red-teaming guidance, NIST will develop companion resources to its (1) AI Risk Management Framework to address generative AI systems, and (2) Secure Software Development Framework to address generative AI systems and dual-use foundation models. The EO also calls for the Department of Homeland Security (DHS) and the Department of Energy to recommend guardrails mitigating the potential for AI to increase critical infrastructure risks, as well as cybersecurity, chemical, biological, radiological and nuclear risks. Relatedly, DHS will establish an Artificial Intelligence Safety and Security Board, which will provide recommendations for improving security related to AI use in critical infrastructure. In addition, the Department of Commerce will develop new guidance for digital content authentication and for watermarking AI-generated content. U.S. federal agencies will use these standards to mark communications that they produce to assist the public in identifying AI-generated digital content produced by the federal government or on its behalf.

Addressing Software Vulnerabilities

The Secretary of Defense and the Secretary of Homeland Security will create a new pilot program to develop AI tools that assist with investigating and addressing vulnerabilities in critical U.S. government software, systems and networks.

AI Use by the Military and Intelligence Community

The National Security Advisor and White House Deputy Chief of Staff for Policy will oversee the development of a National Security Memorandum to provide guidance on the safe and ethical use of AI by the military and intelligence community.

Privacy

Call for Federal Privacy Legislation

Recognizing the inherent limits of an executive order, the Administration explicitly calls on Congress to pass federal privacy legislation to "protect all Americans, especially kids," in a Fact Sheet simultaneously published with the order.

Privacy-Enhancing Technologies (PETs)

The Director of the National Science Foundation (NSF) in conjunction with the Secretary of Energy, will fund a Research Coordination Network (RCN) with the objective of developing standards for deploying privacy-preserving and privacy-enhancing technologies.

Guidance on Use of Personal Information by Federal Agencies

To reduce potential privacy risks from the expansion of AI, the Office of Management and Budget (OMB) will reevaluate how federal agencies use commercially-available information (CAI), including CAI obtained from data brokers, and strengthen privacy guidance for federal agencies.

Civil Rights and Anti-Discrimination

Mitigating AI Risks and Encouraging Responsible Use: New Guidance and Training to Guard Against Discrimination

The Secretary of Housing and Urban Development will issue guidance to prevent the use of AI-enabled tenant screening systems in ways that violate the Fair Housing Act and the Fair Credit Reporting Act. In particular, the guidance will address how the use of credit history and civil and criminal records in the tenant screening process can lead to discriminatory outcomes in violation of federal law.

Criminal Justice System Fairness

To protect against the risk of unlawful discrimination in connection with the criminal justice system's use of AI, the Attorney General will submit to the president a report that addresses the use of AI throughout the criminal justice system, including its use in sentencing, policing and forensic analysis by law enforcement and courts. Within the report, the Attorney General will recommend guidelines for law enforcement agencies, including safeguards and limits for their use of AI. The EO calls for the Attorney General to supplement the report with recommendations to the President, including requests for specific legislation.

Protecting Patients, Students and Workers

Protecting Patients and Students

The EO requires the Department of Health and Human Services (HHS) to establish a safety program to address risks associated with the use of AI in healthcare, including

capturing clinical errors resulting from AI use in healthcare settings, and tracking associated incidents that cause harm, including through AI discrimination. HHS will assess this data to develop guidelines aimed to prevent such harms. In addition, the Secretary of Education will develop an "AI toolkit" for education leaders to implement in the classroom, which will include recommendations for human review of AI decisions, and recommendations for designing AI systems in alignment with privacy laws specific to education (e.g., the Family Educational Rights and Privacy Act).

Supporting Workers

The EO requires the Secretary of Labor, in consultation with other agencies and outside entities, including labor unions, to develop best practices and principles for employers to "mitigate AI's potential harms to employees' well-being and maximize its potential benefits." These practices must address potential job displacement, labor standards, workplace health and safety and workplace data collection.

Promoting Competition, Innovation and American Leadership

Promoting Competition

The EO encourages the Federal Trade Commission (FTC) to consider whether to use its existing rulemaking authority under the Federal Trade Commission Act (e.g., its authority to prosecute unfair and deceptive acts or practices) to ensure fair competition in the AI marketplace and to protect consumers and workers against AI-related harms.

Promoting Innovation

The Administration will support U.S. leadership in AI through the creation of a National AI Research Resource which will aim to broaden access to AI resources and data for researchers and students. The Administration also will expand grants and technical assistance for AI innovation and will encourage AI experts from abroad to work and study in the United States.

Advancing American Leadership Abroad

The Administration expressed its commitment to working with other countries on the development of secure, trustworthy and interoperable AI standards. To that end, the State and Commerce Departments will work with international partners to establish frameworks that seek to advance the benefits of AI while mitigating its risks.

Government Use of AI

Ensuring Responsible and Effective Government Use of AI

Each federal agency will be required to designate a chief AI officer to manage their respective agency's use of AI. In addition, the federal government will issue new guidance for federal agencies' use of AI, procurement of AI solutions and hiring of AI professionals.

Promoting AI Talent

The Biden administration will convene an AI and Technology Talent Task Force which will identify best practices for hiring and retaining AI talent, including diversity, inclusion and accessibility best practices.

NEXT STEPS

The deadlines for federal agencies to fulfill their respective EO obligations vary by agency and sector, ranging from 30 to 540 days from the date of the Order.

The EO is the United States' most sweeping and comprehensive effort to date at regulating AI. Though it primarily applies to federal government agencies, the EO provides insight into the federal government's priorities regarding AI regulation overall. In addition, because the federal government is a major customer of AI systems, the EO will have an indirect effect on developers of AI systems, particularly federal contractors. Because the EO calls for AI-specific guidance and enforcement from a number of different federal regulators across a variety of domains (e.g., consumer protection, education, healthcare, employment, civil rights), private sector companies developing or otherwise using AI should continue to monitor for regulatory developments that arise as a result of the EO.