Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

The AI Executive Order and Considerations for Federal Privacy Policy

January 25, 2024

On October 30, 2023, President Biden issued Executive Order (E.O.) 14110 on *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. This E.O. advances a coordinated approach to the responsible development and use of artificial intelligence (AI) and directs agencies to mitigate privacy risks and bias potentially exacerbated by AI, including "by AI's facilitation of the collection or use of information about individuals, or the making of inferences about individuals."

Since the enactment of the Privacy Act of 1974, the federal government has grappled with how to preserve individual privacy while also leveraging the utility of computerized information. As information resources management transitioned from primarily paper-based materials to digital systems and formats, Congress and the Office of Management and Budget (OMB) have continued to update agency roles, responsibilities, and governance mechanisms with regard to management of agency information.

With expanding use of AI, Congress and the executive branch may explore whether agency roles and responsibilities relating to privacy have kept pace with emerging technologies and information sources. The E.O. describes possible impacts to individual civil liberties and existing privacy protections: "Artificial Intelligence is making it easier to extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires. Artificial Intelligence's capabilities in these areas can increase the risk that personal data could be exploited and exposed." However, advances in privacy-enhancing technologies (PETs) may allow federal agencies to "derive value from, and enable an analysis of, data to drive innovation while also providing privacy and security."

E.O. 14110 represents the continuing discussion concerning federal use of information on individuals and builds upon requirements in the Open, Public, Electronic, and Necessary Government Data Act (OPEN Government Data Act) and the E-Government Act of 2002. The E.O. focuses on three priorities relating to privacy:

1. Identifying and evaluating agency use of commercially available information (CAI);
2. Revising existing privacy requirements for the adoption of AI, including privacy impact assessments (PIAs); and
3. Encouraging agency use of PETs.

Congressional Research Service
https://crsreports.congress.gov
IN12308

Commercially Available Information

Under the Privacy Act, protections regarding the federal use (and recourse for misuse) of individually identifying information center around the information being considered agency records that the agency maintains. However, private entities are not considered "agencies." Observers have questioned what role private entities, such as commercial data brokers, may play in supplementing or comingling with government information and what recourse individuals have in the event of inappropriate use or quality of this third-party information.

The E.O. requires the OMB director to evaluate and identify CAI procured by agencies. CAI is defined as "any information or data about an individual or group of individuals, including an individual's or group of individuals' device or location, that is made available or obtainable and sold, leased, or licensed to the general public or to governmental or non-governmental entities." The E.O. further requires the OMB director to evaluate agency standards and procedures associated with CAI throughout its life cycle, from collection and use of the information to disposition. It is unclear whether this evaluation will require disclosure of the CAI's provenance or origin.

Revising Existing Privacy Requirements

Section 208 of the E-Government Act of 2002 requires PIAs be conducted when agencies develop or procure information technology that collects, maintains, or disseminates information that is in an identifiable form. A PIA includes elements such as what and why the information is being collected, how the information will be secured and shared, and what notice or opportunities for consent are provided to individuals regarding the information collection and sharing. OMB guidance concerning PIAs is largely contained in OMB Circular No. A-130, updated in 2016, and Memorandum M-03-22, published in 2003.

Generally, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. However, agency officials may not share a common understanding of what changes would create new risks, such as the creation or acquisition of a new information system or the updating of an existing system with new information that may change system outputs. Although OMB directs agencies to "conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections" throughout the information life cycle, it is unclear how PIAs are evaluated by non-agency actors who may not fully understand the intended purpose and scope of the information technology being assessed, such as OMB or the public. The E.O. requires the director of the Office of Science and Technology Policy (OSTP) and the assistant to the President for economic policy, in consultation with the Attorney General, to solicit feedback to inform potential revisions to Section 208.

Privacy-Enhancing Technologies

Since the Obama Administration, executive branch policies regarding open government have discussed risks to privacy resulting from access to information in open and machine-readable formats. OMB has described these risks as relating to the *mosaic effect*, where seemingly de-identified information could be collected and re-combined to reveal individuals. Development and adoption of PETs may enable agencies to mitigate privacy harms from the mosaic effect while also providing insights related to program administration and improvement.

In March 2023, components of OSTP released a "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics," suggesting that agency adoption of PETs may be influenced by factors such as

cost and scalability, inconsistent definitions and taxonomy, or tradeoffs between accuracy and utility of the information, among others.

The E.O. provides a broad definition of *privacy-enhancing technology*, which includes any software, hardware, technique, or technological means "of mitigating privacy risks arising from data processing, including by enhancing predictability, manageability, disassociability, storage, security, and confidentiality." The E.O. explains that techniques such as differential privacy, synthetic data generation, and federated learning could be used.

The E.O. requires the creation of a Research Coordination Network dedicated to advancing privacy research, specifically "the development, deployment, and scaling of PETs." Further, it requires the director of the National Science Foundation to engage with agencies to "identify ongoing work and potential opportunities to incorporate PETs into their operations."

Author Information

Meghan M. Stuessy
Analyst in Government Organization and Management

Disclaimer