Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Regulation of Data Brokers: Executive Order 14117 on Preventing Access to Americans' Sensitive Data by Countries of Concern

May 16, 2024

In February 2024, the Biden Administration issued Executive Order (E.O.) 14117 Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern. E.O. 14117 authorizes the Attorney General, in coordination with the heads of other relevant agencies, to issue regulations to prevent the transfer or sale of bulk sensitive personal and government-related data to countries of concern when access would pose an "unacceptable risk to the national security of the United States." The Biden Administration, Congress, and industry and civil society groups have engaged in debates on data security with increased frequency as artificial intelligence (AI) and other data analytics tools increase the potential for exploitation or manipulation of sensitive data.

The Department of Justice (DOJ) issued an Advance Notice of Proposed Rulemaking (ANPRM) to explain its proposed regulations and solicit feedback. The proposed program would cover transactions with countries of concern involving six types of bulk U.S. sensitive personal data (with the definition of "bulk" ranging from 100 to 10,000 U.S. persons, depending on the type of data) and two types of government-related data (regardless of volume) (see **text box**).

Under the proposed program, transactions involving human genomic data and data brokerage transactions involving any type of covered data would be classified as prohibited. Other transactions related to vendor, employment, or investment agreements and involving covered data would be classified as restricted and have to comply with security requirements to be set by the Secretary of Homeland Security. The ANPRM identifies the People's Republic of China (PRC or China), China's Special Administrative Regions of Hong

Covered Data

Bulk U.S. Personal Data

- personal identifiers
- personal financial data
- personal health data
- precise geolocation data
- biometric identifiers
- human genomic data

Government Data

- geolocation data
- sensitive personal data on current or former government employees

Source: ANPRM.

Congressional Research Service
https://crsreports.congress.gov
IN12362

Kong and Macau, Iran, North Korea, Cuba, and Venezuela as countries of concern. The program is to be implemented in stages with exceptions for certain types of cross-border data transactions.

Data Brokerage and Countries of Concern

One of the major sources of access to U.S. citizens and U.S.-government-related data that E.O. 14117 aims to address is the data brokerage industry. Data brokers are broadly defined as firms engaged in the acquisition and sale of data, generally personal data on consumers such as age, location, health conditions, political affiliation, and lifestyle preferences (e.g., travel, purchases). At least one industry expert has found that the large quantities of data for sale on individuals, including active-duty military, may violate civil rights and pose national security risks. One study on data brokers found data brokers employed little to no safeguards to verify the identity of buyers interested in purchasing large quantities of data on military servicemembers, even when the buyer had an IP address in Asia. In an April 2023 hearing on data brokers, one industry expert testified that countries of concern could steal sensitive data from data brokers if such firms do not have adequate data protection in place. For example, PRC hackers gained access to sensitive data on millions of Americans in the 2017 Equifax hack, underscoring the importance of data protection related to collection and storage of sensitive data.

U.S. Policy on Cross-Border Data Flows

E.O. 14117 comes at a juncture in U.S. policy on cross-border data flows when the Administration and some in Congress are reevaluating the benefits and risks of open cross-border data flows. Until 2023, the United States generally supported digital trade policies that promote the free flow of data across borders. The E.O. is one of several actions by the Administration and Congress that represent a change in U.S. policy towards restrictions on cross-border data flows. In 2023, the Biden Administration removed its support for language supporting open cross-border data flows and prohibiting data localization at the World Trade Organization (WTO), citing the need for domestic policy space given shifting debates on technology regulation and other digital economy issues. In April 2024, a supplemental appropriation (P.L. 118-50) became law that contains the Protecting Americans' Data from Foreign Adversaries Act, which prohibits data brokerage transactions with foreign adversaries related to U.S. citizens' personally identifiable sensitive data. The E.O. and these other actions may influence future U.S. digital trade policy, particularly the treatment of cross-border data flows.

E.O. 14117 states that the restrictions are calibrated to minimize the impact on commercial activity, and it does not put in place any data localization requirements. Despite the E.O.'s commitment to an open Internet and the promotion of cross-border data flows that enable trade and investment, cross-border commercial transactions may be impacted, particularly in digital economy sectors such as cloud computing.

Issues Facing Congress

The 118th Congress is considering legislation related to data security and could consider how the aim and implementation of E.O. 14117 overlap with existing or proposed legislation. The Protecting Americans' Data from Foreign Adversaries Act is focused on prohibiting transactions of any volume related to personal data and comes into force 60 days after enactment, while E.O. 14117 covers government-related and bulk personal transactions and builds an implementation program in tranches with no timeline. Congress could consider whether it wants to oversee or be consulted on the DOJ's implementation of the E.O. As part of those efforts, Congress could consider the content of E.O. 14117 (e.g., whether it provides adequate data protection, and covers the appropriate countries of concern, data, and transactions). The United States has not enacted comprehensive federal data privacy legislation. Some Members of Congress

have proposed such legislation, and Congress could assess how such legislation might relate to the goals of the E.O.

Congress could also consider how E.O. 14117 could impact the U.S.'s broader efforts to oversee or regulate the digital economy and the technology sector.

Author Information

Danielle M. Trachtenberg
Analyst in International Trade and Finance

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.