WILMERHALE

Biden Executive Order to Protect Americans' Sensitive Personal Data and Related Rulemaking Could Impose Significant Restrictions on Certain Transfers of Sensitive Personal Information

March 1, 2024

On February 28, 2024, President Biden signed Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern" (the EO), under the authority of the International Emergency Economic Powers Act (IEEPA). Among other things, the EO directs the Department of Justice (DOJ) to issue regulations that prevent the large-scale transfer of certain types of "sensitive personal data" to "countries of concern," including China and Russia. In tandem with the EO, DOJ released an Advance Notice of Proposed Rulemaking (ANPRM) to outline its plan for these regulations.

Although the White House has asserted that the EO will be implemented consistent with the United States's "longstanding support for the trusted free flow of data," DOJ is considering a flat prohibition on two types of transactions between U.S. persons and entities from countries of concern or controlled by nationals of countries of concern: (1) data-brokerage transactions; and (2) transactions involving the transfer of bulk human genomic data. Critically, the ANPRM also contemplates imposing special security requirements and other restrictions on three types of bulk data transactions involving sensitive personal data: (1) vendor agreements involving the provision of goods and services; (2) employment agreements; and (3) investment agreements.

Although the precise timing for a final rule implementing the EO is unclear, the restrictions being contemplated are broad and may create complex diligence and compliance requirements for companies engaged in cross-border data transfers. Of particular note:

- If the DOJ regulations ultimately impose data security requirements on "investment agreements" with countries of concern, every U.S. business that maintains "sensitive personal data" and that takes an investment from a Chinese entity (or entity from any other country of concern) may be subject to new minimum cybersecurity standards.
- DOJ contemplates creating a civil enforcement regime to police compliance with the new data transfer rules. In particular, the ANPRM contemplates a knowledge requirement to establish a violation and states that DOJ is considering whether the failure to develop an adequate due diligence program might be treated as an "aggravating factor" in any enforcement action. At this time, however, the contours of a reasonable, risk-based compliance regime remain unclear. Additionally, because the new regime is premised on presidential authorities created by IEEPA, willful violation of the rules created by the EO may implicate IEEPA's criminal provisions.
- The EO highlights the importance of companies understanding what data they collect, how that data is used, and potential downstream use by third parties. But the details of the regulations have yet to be worked out—including whether and how they will affect domestic and international financial institutions, social media companies, healthcare providers, and others.
- The ability of artificial intelligence (AI) to leverage large datasets for nefarious purposes (or to build new AI models) is a major motivating factor behind the EO. Companies that process personal data need to understand how AI amplifies risks and may expose the business to regulatory scrutiny.
- The U.S. Department of Homeland Security is also directed to propose and seek comments on new security requirements for vendor, employment, and investment agreements. In addition, other agencies, including the Consumer Financial Protection Bureau (CFPB), will issue rules in accordance with this EO, addressing various types of sensitive personal data.
- The EO and ANPRM are natural follow-ons to a partially declassified report released last year, which included several recommendations that the Intelligence Community develop and implement guidance to protect commercially available information. In addition, they appear to be a continuation and amplification of DOJ's increased focus in this area—for example, last year, the DOJ announced a new National Security Cyber Section within the National Security Division, focused on increasing the Department's "capacity to disrupt and respond to malicious cyber activity, while promoting Department-wide and intragovernmental partnerships in tackling increasingly sophisticated and aggressive cyber threats by hostile nation-state adversaries."

Executive Order

The EO and ANPRM illustrate a growing effort by the Administration to aggressively police transactions perceived to empower China and reveal deep concerns about the potential for hostile foreign powers to weaponize bulk data and the power of AI to target Americans. As the EO states:

> Countries of concern can use access to United States persons' bulk sensitive personal data and United States Government-related data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

The White House caveats that this step aligns with the United States's "commitment to an open Internet with strong and effective protections for individuals' privacy and measures to preserve governments' abilities to enforce laws and advance policies in the public interest." Indeed, the EO and ANPRM include exemptions for certain commercial activity—although it remains to be seen how those exemptions will be implemented and how DOJ and others will pursue enforcement.

The White House appears to have considered and rejected the imposition of generalized data location requirements to store Americans' data within the United States, as both the EO and ANPRM explicitly state that this is not the Administration's plan.

Comments on the ANPRM are due by August 26, 2024.

Department of Justice Regulations

The EO directs the DOJ to issue regulations that prohibit or restrict transactions involving (1) "bulk sensitive personal data" or (2) "United States Government-related data," regardless of volume, if it falls within a class of transactions that pose an unacceptable risk to the national security of the United States. The ANPRM describes and seeks comment on a proposed two-tiered regime, in which certain classes of "highly sensitive transactions" would be prohibited, while other classes would be restricted (i.e., permitted only when they comply with predefined security requirements). This regime generally would cover only *knowing* transactions between a U.S. person and a country of concern or covered entity. The ANPRM suggests that rulemaking will occur in phases.

Countries of Concern and Covered Persons

The ANPRM contemplates identifying six "countries of concern": China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela. The proposal is to regulate data transactions between U.S. persons and "covered persons," defined to include certain classes of

entities and individuals subject to the jurisdiction, direction, ownership, or control of countries of concern.

The proposed definition of "covered persons" would extend to those who knowingly cause or direct, directly or indirectly, a violation of the EO or its implementing regulations. As explained in the ANPRM, DOJ intends for the "knowingly" language to apply to persons who knew or should have known of the circumstances of the transaction, taking into account the relevant facts and circumstances, including the relative sophistication of the individual or entity at issue, the scale and sensitivity of the data involved, and the extent to which the parties to the transaction at issue appear to have been aware of and sought to evade the application of these rules. The proposed definition of "covered persons" would *not* include U.S. citizens or people located in the United States.

DOJ is also considering maintaining a public list of persons determined to be covered persons, modeled on various sanctions designation lists maintained by the Office of Foreign Assets Control (OFAC).

Types of Data Covered

The types of data covered are defined by the EO, but DOJ is expected to elaborate on those definitions. "Sensitive personal data" is defined as including "covered personal identifiers, geolocation and related sensor data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof." The definition *excludes* public data, personal communications, and information or informational materials.

The ANPRM elaborates on "covered personal identifiers," noting that the final rule will include a comprehensive list of identifiers, such as government identification numbers, financial account numbers, device-based identifiers, demographic or contact data, advertising identifiers, and more. It likely will not include, for example, employment or criminal history. The ANPRM also proposes to establish volume-based thresholds for these "bulk" transfers using a "risk-based assessment that examines threat[s], vulnerabilities, and consequences as components of risk." Preliminarily, the proposal is as follows:

	Human Genomic Data	Biometric Identifiers	Precise Geolocation Data	Personal Health Data	Personal Financial Data	Covered Personal Identifiers
Low	More than 100 U.S. persons	More than 100 U.S. persons	More than 100 U.S. devices	More than 1,000 U.S. persons		More than 10,000 U.S. persons
High	More than 1,000 U.S. persons	More than 10,000 U.S. persons	More than 10,000 U.S. devices	More than 1,000,000 U.S. persons		More than 1,000,000 U.S. persons

Separately, the EO defines "United States Government-related data" as including (1) geolocation data in listed geofenced areas associated with certain military, other government, and other sensitive facilities and (2) sensitive personal data that is marketed as linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. government, including the military and Intelligence Community. The ANPRM seeks to provide somewhat more detail on these terms.

Covered Data Transactions

DOJ is proposing to define a "covered data transaction" as any transaction that involves (a) bulk U.S. sensitive personal data or (b) Government-related data, regardless of volume, and that involves: (1) data brokerage; (2) human genomic data or human biospecimens from which human genomic data can be derived; (3) a vendor agreement; (4) an employment agreement; or (5) an investment agreement, where "transaction" is broadly defined to be "any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property in which a foreign country or national thereof has an interest." The ANPRM proposes definitions for "access," "data brokerage," "vendor agreement," "employment agreement," and "investment agreement" that are broad and nuanced and may require a significant amount of consideration by companies to understand whether their activities result in participation in covered data transactions.

There are two types of covered data transactions that will be regulated by DOJ. First are prohibited transactions: covered data transactions that are categorically determined to pose an unacceptable risk to national security because they may enable countries of concern or covered persons to access bulk U.S. sensitive personal data or government-related data. The DOJ is initially proposing that these are data brokerage transactions or any transaction that provides a country of concern or covered person with access to bulk human genomic data or human biospecimens from which that human genomic data can be derived. Second are restricted transactions, which are categorically determined to pose an unacceptable risk to national security, because they may enable countries of concern or covered persons to access bulk U.S. sensitive personal data or government-related data ***unless certain security requirements are implemented.***

As to the second category, the ANPRM explains that the security requirements are still under development, but their primary goal will be to address national-security and foreign-policy threats. The current approach contemplated by DOJ is one that permits restricted covered data transactions where the U.S. person (1) implements basic organizational cybersecurity posture requirements; (2) conducts the covered data transaction in compliance with the following four conditions: (a) data minimization and masking; (b) use of privacy-preserving technologies; (c) development of information-technology systems to prevent unauthorized disclosure; and (d) implementation of logical and physical access controls; and (3) satisfies certain compliance-related conditions, such as retaining an independent auditor to perform annual testing and auditing.

The ANPRM also contemplates a licensing regime for transactions that would otherwise be prohibited or restricted. The DOJ is considering permitting both general and specific licenses, which would come with conditions, such as reporting on transactions; these would also involve an interagency consultation process.

Exempt Transactions

Importantly, DOJ is contemplating a series of specific exemptions from these requirements for certain classes of data transactions, including data transactions involving personal communications or informational materials; transactions for the conduct of official business of the U.S. Government; financial-services, payment-processing, and regulatory-compliance-related transactions; intra-entity transactions incident to business operations (e.g., sharing employees' personal identifiers for human resources purposes; payroll transactions to overseas employees); and transactions required or authorized by federal law or international agreements.

These appear to be driven by the Administration's commitment to "promoting an open, global, interoperable, reliable, and secure Internet; protecting human rights online and offline; supporting a vibrant, global economy by promoting cross-border data flows required to enable international commerce and trade; and facilitating open investment." However, it remains to be seen how these exemptions will interact with the thrust of the rule, and whether they will get narrowed during the rulemaking process.

Compliance and Enforcement

The ANPRM explains that the proposed enforcement regime is modeled on OFAC's IEEPA-based economic sanctions program, though there is no strict liability contemplated for violations of the new regulations. U.S. persons would be expected to establish risk-based and reasonable compliance programs, and when a violation occurs, DOJ "would consider the adequacy of the compliance program in any enforcement action." Affirmative due-diligence, reporting, and recordkeeping requirements may only apply to those engaging in restricted transactions or as a condition of a license. The ANPRM also contemplates requiring any U.S. person to keep full records of complete information relative to any covered data transaction subject to a prohibition or restriction.

The DOJ is considering establishing a process for imposing civil monetary penalties similar to the processes followed by OFAC and the Committee on Foreign Investment in the United States (CFIUS), with mechanisms for pre-penalty notice and opportunity to respond, and a final decision.

Homeland Security Requirements

In addition, the EO directs Homeland Security, acting through the Cybersecurity and Infrastructure Security Agency, to propose and eventually publish "security requirements that address the

unacceptable risk posed by restricted transactions." These standards "shall be based on the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology."

Healthcare Requirements

The EO also requires the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation to consider taking steps—including through issuing regulations, guidance, or orders—to prohibit enabling access by countries of concern to Americans' bulk sensitive personal data, including personal health data and human genomic data, or to impose related mitigation measures. The goal here appears to be guarding against the use of federal grants, contracts, and awards for facilitation of access to Americans' sensitive health data by countries of concern.

CFPB Requirements

The EO directs the Director of the CFPB to consider steps to address risks posed by the data brokerage industry in particular, as its members "routinely engage in the collection, assembly, evaluation, and dissemination of bulk sensitive personal data and of the subset of United States Government-related data regarding United States consumers." Director Rohit Chopra has already stated that the CFPB plans to propose new rules focused on corporate data brokers, who are "assembling and selling extremely sensitive data on all of us, including U.S. military personnel, to foreign purchasers."

Other Requirements

The EO also directs the following:

- The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom) shall consider threats to Americans' sensitive data in its reviews of submarine cable licenses. It is directed to issue policy guidance and prioritize reviews of existing licenses for submarine cable systems that are owned or operated by persons owned by, controlled by, or subject to the jurisdiction or direction of a country of concern, or that terminate in the jurisdiction of a country of concern.
- Within one year of the DOJ regulations taking effect, the Attorney General, in consultation with others, is to submit a report—which is to consider public comments—assessing the effectiveness of the measures and the economic impact of the EO.

- Within 120 days of the EO, the Assistant to the President for National Security Affairs, along with many others at the White House and other agencies, shall submit a report to the President assessing the risks and benefits of regulating transactions involving types of human 'omic data other than human genomic data, such as human proteomic data, human epigenomic data, and human metabolomic data.

Interaction with Existing Authorities

DOJ views this EO and ANPRM as building on existing regimes aimed at regulating foreign control of or access to US technology and assets. However, unlike CFIUS and Team Telecom, both of which involve transaction-by-transaction review processes, the ANPRM calls for proscriptive and categorical prohibitions on specified data transfers. Similarly, the Department of Commerce's Information and Communications Technology and Services (ICTS) program focuses on information produced by foreign adversaries and communications technologies and services used in the United States. And while export controls can address the transfer of sensitive products and technologies from the United States to other countries, they do not address the transfer of sensitive personal data.

* * *

We will continue to monitor developments in this area.

Authors

Jason C. Chipman
PARTNER

jason.chipman@wilmerhale.com
+1 202 663 6195

Benjamin A. Powell
PARTNER AND CO-CHAIR, CYBERSECURITY AND PRIVACY PRACTICE; CO-CHAIR, ARTIFICIAL INTELLIGENCE PRACTICE

benjamin.powell@wilmerhale.com
+1 202 663 6770

David J. Ross

PARTNER AND CHAIR, INTERNATIONAL TRADE, INVESTMENT AND MARKET ACCESS PRACTICE GROUP

david.ross@wilmerhale.com

+1 202 663 6515

Arianna Evers

SPECIAL COUNSEL

arianna.evers@wilmerhale.com

+1 202 663 6122

Ariel Dobkin

COUNSEL

ariel.dobkin@wilmerhale.com

+1 202 663 6878