wiley

ALERT

DOJ Kicks Off Work to Regulate Foreign Access to Sensitive Personal Data Under New EO

March 13, 2024

On March 5, 2024, the Department of Justice (DOJ) issued an Advance Notice of Proposed Rulemaking (ANPRM) regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern. The ANPRM follows Executive Order (EO) 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (February 28, 2024), which directed the Attorney General to issue regulations prohibiting or restricting sensitive data transactions with covered countries. Comments are due to DOJ by **April 19, 2024**.

The DOJ's ANPRM proposes (1) prohibitions on covered data transactions, and (2) restrictions on certain covered data transactions. The DOJ is also considering creating a licensing regime that would authorize covered data transactions that would otherwise be prohibited or restricted under the new regulations.

Background

Concern About Artificial Intelligence and Big-Data Analytics Led to the EO and ANPRM

EO 14117 and the DOJ's ANPRM reflect growing concern in government that U.S. adversaries view data as a strategic resource to be exploited to the detriment of U.S. national security. Advanced technologies, including big-data analytics, artificial intelligence (AI), high-performance computing, and other capabilities, are seen as enabling countries of concern to exploit bulk amounts of Americans' sensitive data to achieve these goals. The ANPRM asserts, for

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Daniel P. Brooks
Partner
202.719.4183
dbrooks@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement
Government Contracts
International Trade
National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology

example, that AI is making it easier to extract, re-identify, link, infer, and act on sensitive information about people's identities, location, habits, and desires.[1] Additionally, DOJ says that the combination of personally identifiable information (PII) and large human genomic data sets collected from abroad provides countries of concern with opportunities to precisely target individuals in government or private industries for potential surveillance, manipulation, or exploitation.

Government Sees Risks to National Security

Due to the risk of data exploitation, the ANPRM indicates that certain transactions may enable countries of concern to access bulk amounts of Americans' sensitive personal data and pose an unacceptable risk to national security and foreign policy. The ANPRM asserts that countries of concern can exploit this sensitive data to, for instance, track and build profiles on U.S. persons, including Federal Employees and contractors, military servicemembers, and members of the Intelligence Community, to support espionage operations and to identify and exploit vulnerabilities for malicious cyber activities. Further, the ANPRM notes that countries of concern can also access sensitive bulk information to collect information on activists, academics, journalists, dissidents, political figures, and members of non-governmental organizations and marginalized communities to intimidate opponents of countries of concern, curb dissent, and limit Americans' freedom of expression and other civil liberties.

U.S. Still Remains Committed to Open Trade

Despite these threats, the ANPRM reiterates that the United States remains committed to promoting an open, global, interoperable, reliable, and secure internet; promoting open, responsible scientific collaboration to drive innovation; protecting human rights online and offline; supporting a vibrant, global economy by promoting cross-border data flows to enable international commerce and trade; and facilitating open investment. There have been shifts in the position of the U.S. government, including the rescission last year by the Office of the U.S. Trade Representative (USTR), of its support for e-commerce proposals previously advanced in World Trade Organization (WTO) negotiations. This shift was designed to enable more regulation of data flows by the United States and caused negative reactions from congressional leaders and key industry groups in the digital trade space.

Outline of the ANPRM

The EO Directed the Attorney General to Issue Regulations Identifying Specific Classes of Transactions that Should Be Prohibited or Restricted

EO 14117 directed the Attorney General, in coordination with the Secretary of Homeland Security, to issue regulations identifying specific classes of transactions that may enable access by countries of concern or covered persons to defined categories of Americans' bulk sensitive personal data or government-related data that should be prohibited because that access would pose an unacceptable risk to U.S. national security and foreign policy. The EO also directs the Attorney General to issue regulations identifying specific classes of transactions that will be required to comply with security requirements to be established by the Director of the Cybersecurity and Infrastructure Security Agency (CISA). These security requirements could include:

- Organizational requirements (*e.g.*, basic organizational cybersecurity posture);
- Transaction requirements (*e.g.*, data minimization and masking, use of privacy preserving technologies, requirements for information-technology systems to prevent unauthorized disclosure, and logical and physical access controls); and
- Compliance requirements (*e.g.*, audits).

ANPRM Authorizes the Attorney General to Identify Those Classes of Transactions Likely to be Exploited by Countries of Concern

DOJ issued the ANPRM because it is considering establishing a program that would:

- Identify certain classes of highly sensitive transactions that would be prohibited in their entirety (prohibited transactions); and
- Identify other classes of transactions that would be prohibited except to the extent that comply with predefined security requirements (restricted transactions) to mitigate the risk of access to bulk sensitive personal data by countries of concern.

a. Classes of Restricted Transactions May Include Vendor, Employment, and Investor Agreements

Because they can be significant means by which countries of concern can access sensitive U.S. data, DOJ is considering identifying three classes of restricted data transactions to address critical risk areas involving covered countries, which include:

- Vendor agreements (including agreements for technology services and cloud-service agreements);
- Employment agreements; and
- Investment agreements.

DOJ notes, however, that the national security-related risks with these transactions can be mitigated through appropriate security-related conditions.

b. Sensitive Data May Include PII, Financial, Health, or Location Information

The new DOJ program would cover transactions involving six defined categories of bulk U.S. sensitive data:

- U.S. persons' covered personal identifiers;
- Personal financial data;
- Personal health data;
- Precise geolocation data;
- Biometric identifiers; and
- Human genomic data.

The new program will also cover combinations of these data sets.

c. Volume Is Irrelevant if a Transaction Involves Geolocation Information or Sensitive Information Regarding Current or Former U.S. Government Personnel

The new DOJ program would also address the heightened national security risks posed by U.S. persons' transactions with covered countries regardless of volume if the transaction involves:

- Geolocation data in specific geo-fenced areas associated with certain military, other governmental, or other sensitive facilities (which DOJ states could threaten U.S. national security by revealing information about those locations and U.S. persons associated with them); and
- 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 U.S. military and Intelligence Community.

The new program is intended to address the specific national security threats, including the counterintelligence threats, posed by these specific transactions and, DOJ says, is not intended as a commercial regulation of all cross-border data flows between the U.S. and our foreign partners, nor is the program intended to be a comprehensive program to regulate Americans' data privacy.

What Are the Key Definitions?

Countries of concern would include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela.

Covered persons would include the following:

1. An entity that is at least 50 percent owned, directly or indirectly, by a country of concern, or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;
2. An entity that is at least 50 percent owned, directly or indirectly, by an entity described in category (1) or a person described in categories (3), (4), or (5);
3. A foreign person who is an employee or contractor of a country of concern or of an entity described in categories (1), (2), or (5);
4. A foreign person who primarily resides in the territorial jurisdiction of a country of concern; or
5. Any person designated by the Attorney General as being controlled by or subject to the jurisdiction or direction of a country of concern, or as acting on behalf of or purporting to act on behalf of a country of concern or covered person, or knowingly causing or directing a violation of these regulations.

Covered Data Transaction would be defined as "any transaction that involves any bulk U.S. sensitive personal data or government-related data and that involves: (1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement."

- "Transaction" would be defined as "any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property in which a foreign country or national thereof has an interest."
- "Data brokerage" would be defined as "the sale of, licensing of access to, or similar commercial transactions involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data."
- "Vendor agreement" would be defined as "any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration."
- "Employment agreement" would be defined as "any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level."
- "Investment agreement" would be defined as "as any agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to (1) real estate located in the United States or (2) a U.S. legal entity." The DOJ is considering exemptions to this definition, such as for investments made into publicly traded securities and other passive investments.

Bulk Sensitive Personal Data would include six "sensitive personal data" categories, and the DOJ is proposing certain "bulk" thresholds for each category:

1. "Covered personal identifiers" would include "listed identifiers" that are "linked" to any other "listed identifier," subject to certain exemptions. Covered personal identifiers does not include: demographic or contact data *linked only to another piece of* demographic of contact data; or a network-based identifier, account authentication data, or call-detail data that is *linked only to another* network-based identifier, account-authentication data, or call-detail data for the provision of telecommunications, networking or similar services.
    - The DOJ is proposing a comprehensive list of listed identifiers, which would include, among other things, SSNs, financial account numbers, device-based or hardware-based identifiers (IMEI, MAC addresses, SIM card numbers), demographic and contact data, advertising identifiers (such as Google Advertising ID), account authentication data, network-based identifiers (such as IP addresses or cookie data), and call detail data (such as Customer Proprietary Network Information (CPNI)).
2. "Geolocation and related sensor data."
3. "Biometric identifiers."
4. "Human 'omic data," which would be limited to human genomic data.
5. "Personal health data."

6. "Personal financial data."

Government-related Data builds on definitions from the EO, and the DOJ is considering further defining the term to include two data categories:

1. Any precise geolocation data, regardless of volume, for any location within any area enumerated on a list of specific geofenced areas associated with military, government, or other sensitive facilities or locations; or
2. Any sensitive personal data, regardless of volume, that a transacting party markets 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.

DOJ Looks to Prohibit Covered Data Transactions

The DOJ is considering five potential prohibitions for "covered data transactions":

1. **Prohibition on Covered Data Transactions with Countries of Concern or Covered Persons.** Except as authorized pursuant to an exemption, no U.S. person may knowingly engage in a covered data transaction with a country of concern or covered person;
2. **Contractual Limitations on Data Brokerage Covered Data Transactions with Foreign Persons.** No U.S. person may knowingly engage in a covered data transaction involving data brokerage with any foreign person unless the U.S. person contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving the same data with a country of concern or covered person;
3. **Prohibition on Covered Data Transactions Involving Human Genomic Data.** No U.S. person may knowingly engage in any covered data transaction with a country of concern or covered person that provides that country of concern or covered person with access to bulk U.S. sensitive personal data that consists of human genomic data, or to human biospecimens from which such data could be derived, on greater than [the applicable bulk threshold of] U.S. persons at any point in the preceding twelve months, whether in a single covered data transaction or aggregated across covered data transactions;
4. **Prohibition on Rule Evasions.** DOJ is considering rules that will also prohibit evasions, causing violations, attempts, and conspiracies; and
5. **Further Prohibitions on Rule Evasions.** DOJ is also considering prohibiting U.S. persons from knowingly directing any covered data transaction that would be prohibited (including restricted transactions that do not comply with the security requirements) if engaged in by a U.S. person.

The DOJ is considering creating exemptions from the above prohibitions for:

1. **Intra-entity transactions incident to business operations.** Notably, the DOJ is considering exempting data transactions to the extent that they are: (1) between a U.S. person and its subsidiary or affiliate

located in (or otherwise subject to the ownership, direction, jurisdiction, or control) of a country of concern; and, (2) ordinarily incident to and part of ancillary business operations;

2. **Data transactions involving certain kinds of data**. DOJ would exempt two classes of data transactions to the extent that they involve data that is statutorily exempt from regulation under the International Emergency Economic Powers Act: "personal communications," including any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value, and "information or informational materials";
3. **Official business.** The DOJ would exempt transactions done on behalf of official business of the U.S. Government, including by employees, grantees, contractors, and agencies; and
4. **Financial-services, payment-processing, and regulatory-compliance-related transactions.** The DOJ would exempt certain transactions related to financial services, payment processing, and certain regulations.

Potentially regulated entities should consider whether these exemptions are broad and clear enough to protect routine and important data transfers that may be low risk and candidates for exclusion.

DOJ May Impose Security Requirements on Certain Covered Data Transactions

The DOJ is considering creating classes of restricted covered data transactions that would be prohibited unless they meet certain "security requirements." The subset of covered data transactions would be limited to: (1) vendor agreements; (2) employment agreements; and (3) investment agreements. The security requirements are still "under development," but the DOJ has outlined contemplated security requirements. These could include certain practices drawn from:

- The CISA Cybersecurity Performance Goals (CPGs);
- National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF);
- NIST Privacy Framework (PF); and
- NIST SP 800-171 rev. 3.

In addition, the DOJ has proposed that certain compliance-related conditions, such as retaining an independent auditor, would be needed to satisfy the security requirements. The Department of Homeland Security will seek comment on the security requirements through a separate notice and comment process.

DOJ May Create a Licensing Regime to Permit Some Transactions

The DOJ is considering creating a licensing regime to authorize covered data transactions that would otherwise be prohibited or restricted. The licenses could approve or impose conditions on covered transactions. The DOJ proposes both general and specific licenses. General licenses would authorize certain types of covered data transactions, subject to appropriate terms and conditions. Specific licenses would be applicant-specific, and the DOJ is considering whether to impose requirements that would apply to all specific licensees.

The Government May Offer Interpretive Guidance

The DOJ is considering creating a program to provide guidance through written advisory opinions, which could be requested for any part of the regulations. Additionally, the ANPRM states that DOJ is considering publishing more general interpretive guidance, such as Frequently Asked Questions (FAQs).

DOJ Seeks Input on Compliance and Enforcement Approach

The DOJ is considering certain compliance measures for parties conducting covered transactions, such as risk-based due diligence and recordkeeping requirements, reporting requirements, and independent auditing. The DOJ is also considering establishing a process for imposing civil monetary penalties for violations.

DOJ Is Looking at How Covered Data Transactions May Be Subject to CFIUS Review.

The DOJ is considering how the program should address investment agreements that would also be "covered transactions" subject to the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS). CFIUS reviews covered transactions and can require parties to enter into mitigation agreements or otherwise impose mitigation on a covered transaction to address national security risks. Under the DOJ's proposed program, the rules would not apply to investment agreements that are also covered transactions that have been mitigated by CFIUS. However, if CFIUS's review of a covered transaction concludes without mitigation, then the DOJ's program would still apply.

DOJ Disclaims an Interest in Data Localization

Despite the prohibitions or restrictions on certain bulk data transfers, the ANPRM emphasizes that it is not proposing generalized data localization requirements either to store Americans' bulk sensitive personal data or government-related data within the United States or to locate computing facilities used to process Americans' bulk sensitive data or government-related data within the United States. The new DOJ rules also will not broadly prohibit U.S. persons from concluding commercial transactions with entities and individuals located in countries of concern or impose measures aimed at a broader decoupling of the substantial consumer, economic, scientific, and trade relationships that the U.S. has with other countries. Instead, the ANPRM suggests that DOJ will take calibrated actions to minimize the risks associated with access to Americans' sensitive data while reflecting the U.S. Government's longstanding support of "Data Free Flow with Trust" in recognition of its importance to the economy and human rights online.

***

Wiley's Telecom, Media & Technology and Privacy, Cyber & Data Governance teams, along with the International Trade and National Security practices, have focused on privacy, security, digital trade, data localization, and related issues for decades. This includes advising companies in CFIUS reviews, negotiating data transfer agreements, and supporting compliance with various U.S. and international legal obligations related to the movement and use of data. Whether from a compliance or a policy perspective, our team can address any questions about this EO or the work it has directed.

[1] ANPRM *citing* National Intelligence Council, Assessment: Cyber Operations Enabling Expansive Digital Authoritarianism at 3 (Apr. 7, 2020) (declassified Oct. 5, 2022), https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/3650-cyber-operations-enabling-expansive-digital-authoritarianism.