Foreign Investment & Trade Alert

Weil

April 8, 2024

President Biden Creates Another National Security Program Focused on China and Other Countries of Concern to Limit their Access to Certain Bulk Sensitive Personal Data and U.S. Government-Related Data

By Shawn Cooley, Nathan Cunningham and Christina Carone

On February 28, 2024, President Biden issued an Executive Order (the "EO")[i] establishing a new national security program that would restrict or prohibit certain transactions involving the transfer of specified large-scale sensitive personal data and U.S. Government-related data in order to address national security threats posed by countries of concern that seek to exploit Americans' information. On March 5, 2024, the Department of Justice ("DOJ") issued an Advance Notice of Proposed Rulemaking ("ANPRM")[ii] outlining its plan for yet-to-be-issued implementing regulations (the "Program") that account for concepts set out in the EO. DOJ is seeking comments, which are due by April 19, 2024, from the public on various topics addressed in the ANPRM. The purpose of this new Program is to protect the sensitive personal data of Americans and the U.S. Government from exploitation by countries of concern, which DOJ initially has identified as China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela.[iii] These protections will extend to genomic data, biometric data, personal health data, geolocation data, financial data, and certain personal identifiers.

Key Takeaways

- The Program would be designed primarily to address counterintelligence risks and would prohibit or restrict U.S. persons (and in certain cases foreign persons) from engaging in transactions that involve certain bulk sensitive personal data or U.S. Government-related data with persons from and governments of countries of concern.
- The Program, in effect, disproportionately would impact transactions involving data flows with China (as there are no significant data flows to the other countries of concern as a result of existing sanctions) to protect Americans' most sensitive personal information that bad actors could exploit to the detriment of U.S. national security (*e.g.*, tracking military service members).
- The Program also would have a significant impact on certain data-intensive industries with existing business relationships with China, such as: cloud computing, infrastructure-as-a-service, and advertising. However, every company that maintains or collects in-scope sensitive personal data will be effected by and required to comply with the Program, including those that operate in the healthcare, retail, hospitality, and finance industries.
- Fortunately, existing risk-based economic sanctions or export controls compliance programs could form a basis to implement a similar compliance plan with the Program once it is implemented.

1. Key Concepts and Terms for the Proposed National Security Program

The Program would create an overarching prohibition on in-scope transactions, while contemplating certain broad-based exemptions and permitting other transactions to proceed as long as the parties agree to certain restrictions. As currently constructed, the Program only envisions strictly prohibiting two types of transactions. The Program only would regulate transactions to which a foreign person is a party[iv] and would be comprised of certain key elements, including "Covered Persons," "Covered Data Transactions" and "Sensitive Personal Data."

Only Chinese (including Hong Kong, and Macau), Russian, Iranian, North Korean, Cuban, and Venezuelan persons, their respective governments, and other persons that can be controlled or directed by any such persons or their respective governments, will trigger the Program's jurisdiction (each jurisdiction, a "Country of Concern" and each person, a "Covered Person").

- *Covered Persons*

Generally, the Program would define a Covered Person as being connected in some way to a Country of Concern, including by virtue of majority ownership, control, principal place of business, place of incorporation, employment status, or primary residence. Also, DOJ would have the authority to designate specific persons as Covered Persons, whether because they are owned by, controlled by, subject to the jurisdiction or direction of, acting on behalf of, or purporting to act on behalf of a Country of Concern or other Covered Person, as applicable, or as knowingly causing or directing, directly or indirectly, a violation of the Program.[v,vi] The ANPRM clarifies that a citizen of a Country of Concern that is not primarily resident in a Country of Concern could only constitute a Covered Person if DOJ so designated that person, unless the person worked for the government of a Country of Concern or for another Covered Person, in which case that person would categorically constitute a Covered Person.

- *Covered Data Transaction*

The ANPRM defines a "Transaction" as any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property in which a foreign country or foreign national has an interest.[vii] A "Covered Data Transaction" means any Transaction that involves bulk U.S. sensitive personal data or U.S. Government-related data and that involves (i) a data brokerage agreement, (ii) a vendor agreement, (iii) an employment agreement, or (iv) an investment agreement.

- **Data Brokerage Agreements**: The sale or license of access to data from one person to another person, as long as the recipient had not previously received the data from the person who is the data's source.
- **Vendor Agreements**: Any arrangement, excluding an employment agreement (discussed below), pursuant to which a person provides goods or services to another person in exchange for consideration. Cloud computing services, Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service agreements would all fall under this category.
- **Employment Agreements**: Any arrangement whereby an individual other than an independent contractor, performs work directly for a person in exchange for consideration.
- **Investment Agreements**: Any arrangement pursuant to which any person, in exchange for consideration, obtains direct or indirect ownership interests in or rights related to U.S. real estate or a U.S. legal entity. DOJ is considering excluding from the definition of investment agreement any passive investment that would not provide any interest, rights, or influence that could be used to obtain access to U.S. sensitive personal data or U.S. Government-related data.

The ANPRM specifically mentions the following as examples of passive investments that could be categorically excluded from the Program's jurisdiction as long as they fall below a voting/economic interest threshold and provide no rights beyond standard minority shareholder protections: (i) investments made into a publicly traded security or index fund, mutual fund, or similar arrangement; and (ii) investments made as a limited partner solely into a limited partner structure or equivalent, where the limited partner cannot make managerial decisions, is not responsible for any debts beyond its investment, and does not have formal or informal ability to influence or participate in decision-making or operations.

In each case, DOJ is considering promulgating exemptions, issuing general licenses, and instituting a process for parties to obtain specific licenses.

- *Types of In-Scope Data*

As mentioned above, a Transaction will fall under the Program's jurisdiction only if it involves U.S. persons' sensitive personal data in amounts above certain enumerated thresholds (*i.e.*, "bulk" data) or if it involves certain U.S. Government-related data.

- *Sensitive Personal Data*

The EO defines ''Sensitive Personal Data'' as ''covered personal identifiers, geolocation and related sensor data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof . . . that could be exploited by a Country of Concern to harm United States national security if that data is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals."[viii]

The ANPRM provides for six categories of Sensitive Personal Data along with proposed thresholds, below which the data would not be regulated by the Program:

- Covered personal identifiers only to the extent that one covered personal identifier is linked to another covered personal identifier, except for (i) demographic data that is linked only to other demographic data and (ii) telecommunications data (*i.e.*, account authentication data, network-based identifier data, and call-detail data) linked only to other telecommunications data as necessary for the provision of telecommunications or networking services:
  - Government identification or account numbers;
  - Financial account or personal identification numbers;
  - Device- or hardware-based identifier numbers (*e.g.*, International Mobile Equipment Identity (IMEI), Media Access Control (MAC), or Subscriber Identity Module (SIM) numbers);
  - Demographic or contact data (*e.g.*, first and last name, birth date, zip code);
  - Advertising identifier (*e.g.*, Google ID, Apple ID); and
  - Telecommunication data:
    i. Account authentication data (*e.g.*, account username, account password);
    ii. Network-based identifier data (*e.g.*, IP address, cookie data); and
    iii. Call-detail data (*e.g.*, customer proprietary network information).[ix]
- Geolocation and related sensor data that can identify the physical location of an individual or a device within a prescribed distance;[x]
- Biometric identifiers (*e.g.*, facial images and finger prints);[xi]

- Human genomic data (*i.e.*, data representing the nucleic acid sequences that comprise the entire set or a subset of the genetic instructions found in a human cell, including the results of an individual's genetic test and any related human genetic sequencing data);[xii]
- Personal health data (*i.e.*, individually identifiable health information);[xiii] and
- Personal financial data (*i.e.*, data regarding an individual's credit card or bank account, data in a financial statement).[xiv]

For each of the above, DOJ is considering instituting thresholds, under which the Program would not regulate the data, ranging from data of more than 100 U.S. persons to data of more than 1,000,000 U.S. persons, depending the category. DOJ is also proposing to include combined data sets containing data of more than one of the types above, or geolocation, biometric, human genomic, personal health, or personal financial data if linked to a covered personal identifier, as long as in each case the lowest threshold applicable to the present data is satisfied.

Of note, the ANPRM does not exclude anonymized or de-identified data. The ANPRM also does not exclude the personal data of employees maintained by their employer, in contrast to CFIUS' definition of sensitive personal data.

- *U.S. Government-Related Data*

The EO defines "U.S. Government-related data" as Sensitive Personal Data that, regardless of volume, the Attorney General determines poses a heightened risk of being exploited by a Country of Concern. The EO defines U.S. Government-related data as data that is (i) linked or linkable to former senior officials or categories of current or recent former employees or contractors of the U.S. Government; (ii) linked to categories of data that could be used to identify former senior officials or current or recent former employees or contractors of the U.S. Government; or (iii) geolocation data that is linked or linkable to certain sensitive locations, the geographical areas of which will be specified publicly, that are controlled by the U.S. Government.

The ANPRM contemplates limiting U.S. Government-related data to either (i) Sensitive Personal Data that a transacting party markets as linked or linkable to certain current or former U.S. Government officials, employees, or contractors or (ii) geolocation data for a location within an enumerated area contained on a forthcoming list of U.S. Government facilities. Notably, pursuant to this approach, Sensitive Personal Data that is linked or linkable to current or former U.S. Government officials, employees, or contractors, but that is not marketed by a transacting party as being so linked or linkable would be outside the scope of this definition. The described U.S. Government geolocation data also does not need to be linked or linkable to any individual, rather, these data merely must be linked or linkable to an enumerated U.S. Government location.

2. Prohibited Transactions

The ANPRM's prohibited transactions involve interrelated concepts and definitions, including the definition of a Covered Data Transaction, Covered Person, and Sensitive Personal Data. The Program's two categorical prohibitions are the focus of the ANPRM and represent DOJ's attempt to regulate the highest risk data transactions from a national security perspective. The Program also would implement an overarching prohibition subject to authorized exemptions. In addition, the ANPRM would prohibit a U.S. person from evading the Program and from knowingly directing a Transaction that would be prohibited for a U.S. person to undertake.

At least for now, the categorical prohibitions on certain Covered Data Transactions exist separate and apart from restricted or exempted Covered Data Transactions, which are discussed below.

- *Prohibition 1: Data Brokerage Transactions*

The ANPRM would prohibit a U.S. person from knowingly undertaking a data brokerage Transaction with any foreign person (as distinct from a Covered Person) unless the foreign person contractually agrees not to engage in a subsequent Covered Data Transaction with a Covered Person involving the same data. This is the only instance in which the Program would regulate a Transaction to which a U.S. person is not a party.

- *Prohibition 2: Human Genomic Data Transactions*

The ANPRM would prohibit a U.S. person from knowingly undertaking a Covered Data Transaction with a Covered Person that provides that Covered Person access to human genomic data, or to the biospecimens from which such data could be derived, on greater than the applicable threshold at any point in the previous twelve months, whether as a result of one or more Covered Data Transactions.

3. Exempted Transactions

The ANPRM contemplates exemptions that would mirror the exemption of prohibited transactions in the context of the Office of Foreign Asset Controls of the U.S. Treasury Department's ("OFAC") administration of economic sanctions regulations. The ANPRM mentions that these exemptions could pertain to financial services, personal communications, informational materials, U.S. Government official business, regulatory compliance, and intra-company Transactions. Consistent with OFAC's approach taken in the economic sanctions context, these exemptions would exist separate and independent from any general or specific licenses that DOJ issues to engage in an otherwise prohibited Transaction.

The ANPRM contemplates that the financial services exemption would encompass any Transaction that is ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or that is required for compliance with federal financial services laws or regulations. Federally certified national banking associations, and Transactions that are financial in nature, incidental to a financial activity, or complementary to a financial activity will be exempt as well. In addition, the provision or processing of payments involving the transfer of Sensitive Personal Data, including clearing and settling electronic payments and securitizing and selling asset-backed obligations, would be exempt as long as they do not involve data brokerage.

The EO authorizes DOJ to exempt additional classes of transactions, and the full scope of the Program's exemptions should emerge as DOJ's rule making progresses.

4. General & Specific Licenses

DOJ's contemplated approach for issuing general and specific licenses also will mirror OFAC's approach. Licenses issued under the Program will approve some Transactions and in other cases will impose conditions that must be satisfied in order for the Transaction to be authorized. The ANPRM contemplates that DOJ will have the authority to issue general and specific licenses with respect to both prohibited and restricted Transactions. The Program could require that a beneficiary of a general or specific license file reports or statements with DOJ, or provide certain assurances to DOJ related to deleting or safeguarding the relevant Sensitive Personal Data.

5. Restricted Transactions

The ANPRM mentions as a general principle that the Program will establish a subset of Covered Data Transactions, constituting employment agreements, vendor agreements or investment agreements, that will not be prohibited if the parties adhere to certain restrictions. While DOJ is still developing the particular restrictions, the ANPRM anticipates that established cyber security standards and practices, certain access controls and privacy technology, and annual testing and auditing would be elements of the Program's restrictions. Notably, the ANPRM contemplates only prohibiting data brokerage transactions, and does not list data brokerage transactions as within the contemplated scope of restricted transactions. This suggests that if a data brokerage transaction were to constitute a Covered Data Transaction, it would be strictly prohibited and would not be eligible to proceed under any restrictions imposed by the Program on the parties.

6. Compliance Programs & Other Notable Aspects

DOJ is considering implementing a compliance and enforcement program modeled on the Department of Treasury's economic sanctions administered by OFAC. As such, U.S. companies with Sensitive Personal Data or U.S. Government-related data should expect to implement compliance programs, which should be able to leverage much of the framework of existing economic sanctions and export controls compliance programs. In developing a compliance program, companies should (i) account for business and industry-specific risks; (ii) review existing agreements involving the sale of data to other parties (*e.g.*, advertisers and marketers) and consider updating those agreements to identify the final destination of the Company's data; (iii) appreciate the data they are making available, and to whom; (iv) account for the business practices of counterparties (*e.g.*, data brokers) related to direct and indirect data sales; and (v) have a thorough understanding of their data sales (*e.g.*, understand the data categories and how much data is involved in transactions). Companies that proactively inquire into these aspects will be in a better position when the final rule takes effect. Covered Data Transactions that would be restricted or that would be authorized pursuant to general or specific licenses may have their own compliance requirements.

As DOJ's rule making progresses pursuant to the EO and the ANPRM, we expect DOJ to provide further details on the classes of restricted transactions and the classes of exempt transactions.

While DOJ does not intend for the Program to overlap significantly with other legal authorities, the ANPRM acknowledges that there could be a potential overlap with CFIUS' jurisdiction with investment agreements that are also Covered Data Transactions. To resolve this overlap, the ANPRM contemplates that the Program would not have jurisdiction over a Transaction if CFIUS has required the parties to execute a national security agreement with respect to that Transaction, or has otherwise imposed mitigation. Absent a national security agreement or other mitigation, the Program would retain jurisdiction over the Transaction even if CFIUS has already reviewed it and did not require the parties to execute a national security agreement.

The public may submit comments on various topics related to the implementation of the EO through April 19, 2024. The Attorney General is expected to publish in the Federal Register the proposed rule by or about August 26, 2024 (*i.e.*, within 180 days of the publication date of the EO), triggering another round of public comments. DOJ has stated publicly that it expects the Program to be effective around the first or second quarter of 2025.[xv]

* * *

If you have questions concerning the contents of this alert, or would like more information, please speak to your regular contact at Weil or to the authors:

Authors

Shawn Cooley (D.C.)	View Bio	shawn.cooley@weil.com	+1 202 682 7103
Nathan Cunningham (D.C.)	View Bio	nathan.cunningham@weil.com	+1 202 682 7156
Christina Carone (D.C.)	View Bio	christina.carone@weil.com	+1 202 682 7258

[i] Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, 89 Fed. Reg. 15421 (Published March 1, 2024), available here. *See also* FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data (February 28, 2024), available here.

[ii] Official ANPRM: National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern (Published March 5, 2024), available here. DOJ is seeking comments, which are due by April 19, 2024, from the public on various topics related to the implementation of the EO. Following review of the comments received in response to the ANPRM, DOJ will conduct all required analyses (by statute or the EO) for the notice of proposed rulemaking required to implement the EO. The Attorney General, in coordination with the Secretary of Homeland Security, and in consultation with the heads of relevant agencies, is expected to publish the proposed rule by or about August 26, 2024 (*i.e.*, within 180 days of the publication date of the EO).

[iii] *See id.*

[iv] The ANPRM does not address restricted data transactions in significant detail because DOJ and the Department of Homeland Security are still developing the applicable requirements. It is possible that the Program will restrict Covered Data Transactions to which a Covered Person is not a party if that Covered Person is owned, controlled, or affiliated with the foreign person who is the party to the Transaction. However, the ANPRM does not provide any insight in this regard.

[v] The ANPRM states that a Covered Person would be: (1) An entity that is 50% or greater owned, directly or indirectly, by a Country of Concern or that is organized under the laws of or has its principal place of business in a Country of Concern; (2) An entity that is 50% or greater owned, directly or indirectly, by any of the persons described in 1, 3, 4, and 5 herein; (3) A foreign person who is an employee or contractor of any of the persons described in 1, 2, or 5 herein; (4) A foreign person who is primarily resident in a Country of Concern; and (5) A person designated by the Attorney General as being owned or controlled by, subject to the jurisdiction or direction of, or acting or purporting to be acting on behalf of a Country of Concern, or who is knowingly causing or directing a violation of the Program.

[vi] OFAC's 50 Percent Rule imposes sanctions on companies with combined ownership by sanctioned parties of 50% or more. Additional information is available here.

[vii] This definition closely follows OFAC's language prohibiting transactions with specially designated nationals, which effectively prohibits a U.S. person from transferring, paying, exporting, withdrawing, or otherwise dealing in any property or interest in property of a specially designated national. *See, e.g.*, Exec. Order No. 14,065, 87 Fed. Reg. 10293 (Feb. 23, 2022).

[viii] "Sensitive personal data" means "covered personal identifiers, geolocation and related sensor data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof that could be exploited by a country of concern to harm United States national security if that data that is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals." "Data that is a matter of public record" and certain personal communications and information within the scope of the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) ("IEEPA") are excluded from this definition

[ix] "Covered personal identifiers" means personally identifiable data that is reasonably linked to an individual or could be used with other data to identify an individual from a data set or to link data across multiple data sets to an individual, subject to exclusions.

[x] "Geolocation and related sensor data" means limited to precise geolocation information (*i.e.*, data, whether real-time or historical, that identifies the physical location of an individual or device to an exact level of precision based on electronic signals or inertial sensing units).

[xi] "Biometric identifiers" means measurable physical characteristics or behaviors used to recognize or verify the identity of an individual.

[xii] Both the EO and the ANPRM define "human genomic data," with the ANPRM clarifying aspects of the EO's definition. While the EO provides DOJ the authority to regulate all human 'omic data, the ANPRM states that DOJ currently intends for its first rulemaking to regulate human 'omic data only to the extent it constitutes "human genomic data". The EO defines "human 'omic data" as data generated from humans that characterizes or quantifies human biological molecule(s) (*e.g.*, human genomic data, proteomic data, transcriptomic data, epigenomic data, or metabolomic data, or microbiomic data).

[xiii] "Personal health data" means "individually identifiable health information," regardless of whether such information is collected by a "covered entity" or "business associate," as those terms are defined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the HIPAA Privacy Rule; individually identifiable health information includes certain demographic information (*e.g.*, information received by a health care provider that relates to a present mental health condition of an individual and identifies the individual).

[xiv] "Personal financial data" means data concerning an individual's credit, charge, or debit card, or bank account.

[xv] Eric Johnson, Principal Deputy Chief, Foreign Investment Review Section of DOJ's National Security Division, stated during an episode of "Ten Minutes On" that DOJ anticipates publication of the final rule within a year. The episode is available on Foreign Investment Watch.