U.S. Acts to Limit Export of Sensitive Personal Data

March 18, 2024

On February 28, 2024, U.S. President Joe Biden signed Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the "Order"). Concurrently with the issuance of the Order, the U.S. Department of Justice ("DOJ") released an Advance Notice of Proposed Rulemaking ("ANPRM") that discusses the potential regulatory framework to implement the Order (the "Program"), providing over 50 examples of how the Program might be implemented and seeking public comment on over 100 questions by April 19, 2024.[1]

As discussed in our earlier blog post, the Order finds that efforts by certain "countries of concern" to access sensitive personal data constitute an "unusual and extraordinary threat … to the national security and foreign policy of the United States." Under current law, this data may be legally obtained by such parties through data brokerages, third-party vendor agreements, employment agreements, investment agreements or similar arrangements. However, DOJ expresses concern that this digital footprint can be exploited by countries of concern, using technologies including artificial intelligence ("AI"), for purposes of malicious activities (*e.g.*, espionage, coercion, and blackmail). These risks were highlighted yet again over the past week with renewed concerns about TikTok. In an attempt to mitigate these national security concerns, the Order authorizes the Attorney General to take actions to prevent high-volume transfer of Americans' personal data, or transfers of certain U.S. Government data, to countries of concern. Our understanding is that DOJ is truly interested in feedback from the community and encourages that feedback to modify the proposal.

[1] National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 Fed. Reg. 15780 (Mar. 5, 2024).

Key Points of the Proposal

Legal Obligations

First, and foremost, the Order and the ANPRM do not establish immediate restrictions or legal obligations. Rather, the ANPRM represents an initial step in what is likely to be a long regulatory process, likely lasting at least through this year, of framing and defining the limits set forth in the Order. Once comments are received on the ANPRM, DOJ will need to consider them and then issue a Notice of Proposed Rulemaking, likely in late August 2024, which will be subject to a further notice and comment period. Given this process, companies and individuals will be required to comply only when the final rule becomes effective.

Prohibitions

The ANPRM contemplates five prohibitions:

- Knowingly engaging in a covered data transaction with a country of concern or covered person.
    - The knowledge requirement means that this prohibition will not operate under a strict liability standard, although common compliance principles regarding undertaking reasonable risk assessments and avoiding "willful blindness" likely would be relevant.
- Undertaking data-brokerage transactions involving the transfer of bulk U.S. sensitive personal data or government-related data to countries of concern or covered persons.
- Undertaking covered data transactions involving access by countries of concern to U.S. persons' bulk human genomic data or human biospecimens from which human genomic data can be derived.
- Knowingly directing any covered data transaction that would be prohibited if engaged in by a U.S. person, including restricted transactions that do not comply with the security requirements discussed below.
- Evading these restrictions or causing a US person to violate their own obligations.

Key Definitions

The Order and ANPRM propose to restrict or prohibit U.S. persons from engaging in "covered data transactions" that transfer "bulk" amounts of "sensitive personal data" or "U.S. government-related data" to a "covered country or person." Each of these key terms will require definition, and DOJ has sought comment on the scope of these terms.

Covered Data Transactions. The Order broadly defines "transactions" as "any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest."

The ANPRM further defines "covered data transactions" regulated by the Program as "transactions" that involve bulk U.S. sensitive personal data or government-related data in the context of: (1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement. The Program would distinguish between prohibited transactions that are highly sensitive, posing national security risks that are not mitigatable, and restricted transactions that would pose unacceptable risks to national security unless security requirements are implemented. The definition also includes several key exemptions for data transactions, as discussed below.

- As noted above, data-brokerage transactions and transactions involving the transfer of bulk human genomic data would be *prohibited* altogether.

- Three other types of data transactions would be *restricted* under the ANPRM: (1) vendor agreements (including cloud-service agreements); (2) employment agreements; and (3) investment agreements. These transactions would be subject to security requirements that are expected to be based on existing standards, as discussed in our blog post. These security requirements will be published by the Department of Homeland Security in coordination with DOJ.

Sensitive Personal Data. "Sensitive personal data" is defined in the Order to include the six categories of data identified below and combinations of these data that could be exploited by a country of concern, harming U.S. national security if this data is linked or linkable to an identifiable American individual or to a discrete and identifiable group of American individuals (but excludes public record data and data exempt under IEEPA, as discussed below).

The six categories are:

- **Covered Personal Identifiers**. The final rule will include a comprehensive list of identifiers that would include classes of data that are reasonably linked to an individual that could be used to identify an individual. DOJ anticipates that this list

would include data such as a full or truncated government identification or account number (including a Social Security Number), contact data (such as names and addresses), network-based identifier (like an IP address), account-authentication data (including an account password) and call-detail data. DOJ also anticipates excluding certain types of information from the definition, such as employment or criminal history.

- **Geolocation and Related Sensor Data**. The ANPRM explains that DOJ intends to regulate only geolocation and related sensor data to the extent that such transactions involve precise geolocation data, meaning data, whether real-time or historical, that identifies the physical location of an individual or a device with a certain precision (measured by meters or feet).

- **Biometric Identifiers**. The ANPRM defines biometric identifiers to mean "measurable physical characteristics or behaviors used to recognize or verify the identity of an individual." This would include, for example, facial images, voice patterns, retina scans and fingerprints.

- **Human 'omic Data**. DOJ explains in the ANPRM that it intends for the rulemaking to regulate human 'omic data only to the extent that covered data transactions involve human genomic data, including the result or results of an individual's "genetic test" (as defined in 42 U.S.C. 300gg-91(d)(17)) and any related human genetic sequencing data.

- **Personal Health Data**. The term personal health data means, as defined in the ANPRM, "individually identifiable health information" (as defined in 42 U.S.C. 1302d(6) and 45 CFR 160.103), regardless of whether such information is collected by a "covered entity" or "business associate" (as defined in 45 CFR 160.103).

- **Personal Financial Data**. This term is defined in the ANPRM to include "an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities and debts, and transactions" or data in a credit or consumer report.

Bulk Thresholds. The Program will generally regulate sensitive personal data only if the transactions exceed certain bulk volumes (i.e., a threshold number of U.S. persons or U.S. devices). DOJ seeks comment on various aspects of the bulk thresholds but is considering bulk thresholds that vary based on the category of sensitive personal data within the ranges in the table below, based on its preliminary risk assessment.

	Human genomic data	Biometrics 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* (for *biometric identifiers*) or *U.S. devices* (for *precise geolocation data*).		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* (for *biometric identifiers*) or *U.S. devices* (for *precise geolocation data*).		More than 1,000,000 *U.S. persons*.		More than 1,000,000 *U.S. persons*.

U.S. Government-Related Data. The Program also would regulate data transactions involving "U.S. government-related data," defined in the Order as sensitive personal data that poses a heightened national security risk, regardless of volume, and is linkable to either senior government officials or sensitive federal government locations.

In the ANPRM, DOJ explains that it is considering further refining this definition to include two categories: (1) precise geolocation data for certain sensitive government facilities included on a "Government-Related Location Data List" that would be created by an interagency process; or (2) any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or former U.S. government officials, employees or contractors. Unlike the "sensitive personal data" restrictions, the restrictions on U.S. government-related data are not subject to any volume thresholds.

Covered Countries of Concern. The ANPRM contemplates identifying six countries of concern: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela.

Covered Persons. Covered persons would include certain types of entities and individuals whom, as a practical and legal matter, providing data to would effectively give access to the countries of concern. Exceptions are proposed for U.S.-based persons.

- The Order defines categories of covered persons as: (1) "an entity owned by, controlled by, or subject to the jurisdiction or direction of a country of concern"; (2) "a foreign person who is an employee or contractor of such an entity"; (3) "a foreign person who is an employee or contractor of a country of concern"; (4) "a foreign person who is primarily resident in the territorial jurisdiction of a country of concern"; or (5) persons designated by the Attorney General.

- DOJ discusses specific guidance in determining a covered person and contemplates that the Program would identify a covered person as a person that either falls into

one of certain classes or is individually designated by DOJ on a public list, modeled on sanctions designations lists maintained by OFAC.

Exclusions

The Program would exempt certain data transactions from regulation if they fall under a category discussed below. DOJ is considering exempting classes of data transactions, mirroring OFAC's approach in IEEPA-based sanctions regulations.

Data Transactions Exempt from IEEPA. The Program excludes personal communications that are within the scope of section 203(b)(1) of IEEPA (including postal, telegraphic or telephonic communication, which do not involve a transfer of anything of value); and information or informational materials within the scope of section 203(b)(3) of IEEPA (including, for example, publications, films, posters, photographs and news wire feeds). We note that, as discussed below, these IEEPA restrictions have previously been considered, and read broadly, by courts in similar circumstances.

Financial-Services, Payment-Processing and Regulatory-Compliance-Related Transactions. The Order exempts data transactions that are ordinarily incident to and part of the provision of financial services, including banking, capital markets and financial insurance services, or transactions required for regulatory compliance, which are further defined in the ANPRM.

Intra-Entity Transactions Incident to Business Operations. DOJ is also considering exempting transactions between a U.S. person and its subsidiary or affiliate located in a country of concern that are ordinarily incident to and part of ancillary business operations, such as payroll transactions.

Official Business Transactions. The Order exempts data transactions that are part of the activities of the U.S. government, its employees, contractors or grantees, or transactions conducted pursuant to a U.S. government contract.

Transactions Required or Authorized by Federal Law or International Agreements. The ANPRM also contemplates exempting data transactions required or authorized by federal law or international agreements, such as passenger-manifest information, INTERPOL requests or public health information.

Whole-of-Government Approach

The Order is designed to be a "whole-of-government" approach, with significant roles through interagency consultation requirements for the Departments of State, Commerce, Treasury, Homeland Security and other agencies. The Order also directs

certain agency actions to address data security risks associated with countries of concern with regard to: (1) submarine cable systems (delegated to the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector ("Team Telecom")); (2) grantmaking and contracting authorities related to sensitive health data and human genomic data (delegated to the Departments of Defense, Health and Human Services, and Veterans Affairs, and the National Science Foundation); and (3) the role of data brokers (delegated to the Consumer Financial Protection Bureau).

Penalties

The Order authorizes DOJ to investigate violations of the regulations, including pursuing civil and criminal remedies available under IEEPA, which currently carry a maximum civil penalty per violation of the greater of $368,136 or an amount that is twice the amount of the underlying transaction, and, for willful violations, may incur criminal penalties of $1 million per violation and, for individuals, up to 20 years imprisonment per violation. The ANPRM also contemplates establishing an enforcement process to impose civil penalties for violations, similar to civil enforcement processes at other regulators, such as OFAC.

Interaction with Other Authorities

In the ANPRM, DOJ considers how the Program might interact with existing authorities, particularly the Committee on Foreign Investment in the United States ("CFIUS"), and specifically seeks comment on this issue. DOJ does not anticipate that the Program will have significant overlap with existing authorities, which are not prospective and categorical. In particular, unlike the case-by-case reviews of the CFIUS regime, DOJ will establish generally applicable rules to implement the Program. However, for investment agreements between U.S. persons *and* countries of concern (or covered persons) that are also "covered transactions" which are subject to CFIUS review, DOJ contemplates an approach in which the Program would independently regulate these transactions until CFIUS takes action to enter into or impose mitigation measures to address national-security risk arising from a covered transaction.

Takeaways

DOJ described the Program as a "groundbreaking" step to protect Americans' personal data. U.S. restrictions on the export of Americans' personal data would be similar to (but less strict than) other regimes worldwide that prohibit the export of domestic personal data. DOJ took great pains to argue that the proposed rules were not a "data localization" regime and that the U.S. continued to advocate for the free flow of data across borders.

Below, we discuss reactions and potential issues that may arise in implementing the Program.

- The Program would require companies to create risk-based compliance programs, such as the ones they currently use to comply with economic sanctions, with meaningful civil and criminal penalties for violations. Given the intentional similarities between the IEEPA-based sanctions regulations, companies may be able to leverage similar, risk-based compliance approaches to comply with a future rule.

- As discussed in our blog post regarding the Program, companies may wish to begin now to consider what enhancements to existing diligence processes, security controls, changes to existing agreements (including vendor agreements) and compliance audit processes may be needed. Companies also may wish to begin a data mapping process to identify the sensitive personal data and U.S. government-related data that they hold and where that data is stored and processed.

- As noted above, the Order excludes from the definition of sensitive personal data personal communications that are within the scope of section 203(b)(1) of IEEPA and information or informational materials within the scope of section 203(b)(3) of IEEPA. The ANPRM asks for comment on how DOJ should define "information" and "informational materials" for purposes of this exemption and suggests that the regulations may propose to exclude only "expressive information" under this exemption.

    - On that point, in earlier attempts by the U.S. government to impose restrictions regarding U.S. personal information under IEEPA-based executive orders, several federal courts were not convinced of the U.S. government's arguments that the proposed restrictions were consistent with IEEPA's exclusion for information and informational materials, with several federal courts finding that those efforts' functional restriction on the export of information or informational materials, regardless of the government's purpose in adopting those controls, likely fell outside of IEEPA's authorization.[2] It is unclear whether DOJ's proposed distinction between "expressive information" (excluded) and other "information" (regulated) would be authorized under IEEPA.

- It is possible that a final rule could change approach, including after adoption, to account for concerns that the Program's "targeted" approach may be too narrowly

---

[2] See *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92, 108 (D.D.C. 2020), *appeal dismissed sub nom. TikTok Inc. v. Biden*, No. 20-5381, 2021 WL 3082803 (D.C. Cir. 2021), *available* here; *Marland v. Trump*, 498 F. Supp. 3d 624, 641 (E.D. Pa. 2020), *available* here.

> construed to effectively block the commercial transfer of U.S. data to countries of concern, leaving gaps that allow countries of concern to create workarounds. For example, any "bulk" threshold restriction could be circumvented by transferring data in smaller denominations. Further, as the Order notes, countries of concern can use AI and algorithms in sophisticated ways to identify patterns across multiple unrelated datasets, de-anonymizing or re-identifying data, or might transform data to disguise its original identification.[3]

With comments on the ANPRM due on April 19, 2024, industry participants and their trade associations will take steps to assess the impact that the Order and forthcoming regulations may have on their data management and their dealings in China and other countries of concern. As noted above, we expect many to comment on the ANPRM. Subsequently, consistent with the Order, we would expect DOJ to issue a proposed rule by August 26, 2024 (within 180 days of the date of the Order).

* * *

We will continue to monitor developments and provide additional updates as warranted.

Please do not hesitate to contact us with any questions.

Satish M. Kini
Partner, Washington, D.C.
+1 202 383 8190
smkini@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Rick Sofield
Partner, Washington, D.C.
+1 202 383 8054
rcsofield@debevoise.com

---

[3] For instance, research has demonstrated, using credit card metadata, that just four random pieces of information were enough to re-identify 90% of anonymized shoppers as unique individuals. Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010, U of Colorado Law Legal Studies Research Paper No. 9-12, Available at SSRN: https://ssrn.com/abstract=1450006. "Researchers Use Big Data And AI To Remove Legal Confidentiality," (Sep. 19, 2019) Forbes, available at https://www.forbes.com/sites/simonchandler/2019/09/04/researchers-use-big-data-and-ai-to-remove-legal-confidentiality/?sh=5383d7bc15f6; https://www.nature.com/articles/s41467-019-10933-3. *See also, e.g.,* Washington Post, Candidates and Super PACs Can't Coordinate, Here's Their Workaround (Mar. 11, 2014), available at https://www.washingtonpost.com/news/the-fix/wp/2014/03/11/candidates-and-super-pacs-cant-coordinate-heres-their-silent-workaround/.

Robert T. Dura
Counsel, Washington, D.C.
+1 202 383 8247
rdura@debevoise.com

Taylor Richards
Associate, Washington, D.C.
+1 202 383 8009
tmrichards@debevoise.com

Stephanie D. Thomas
Associate, New York
+1 212 909 6535
sdthomas@debevoise.com

Yair Strachman
Law Clerk, New York
+1 212 909 7477
ystrachman@debevoise.com