MAYER | BROWN

MARCH 05, 2024

PRESIDENT BIDEN ISSUES EXECUTIVE ORDER EMPOWERING DOJ TO REGULATE THE EXPORT OF SENSITIVE PERSONAL DATA

AUTHORS: AARON FUTERMAN, ADAM S. HICKEY, HOWARD W. WALTZMAN

On February 28, 2024, President Joe Biden issued Executive Order ("EO") 14117 , empowering the Department of Justice (DOJ) to regulate the export of certain consumer data, in order to prevent certain countries' governments from obtaining bulk sets of especially sensitive personal data. The EO, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," addresses longstanding concerns from the Executive Branch that certain foreign governments are amassing sensitive genomic, biometric, health, geolocation, financial, and other personal data and using it to engage in activities that threaten national security, such as espionage (including through computer hacking), blackmail, transnational repression, and disinformation campaigns.

As a first move, the EO aims to close the "front door" that allows data brokers and other commercial actors to sell large sets of sensitive personal data to particular foreign governments, by prohibiting certain transactions outright. But DOJ contemplates a broader set of regulations of vendor, employment, and investment agreements that may give foreign companies from countries of concern (and *ipso facto* those governments) indirect access to sensitive personal data. The White House and DOJ perceive the restrictions likely to emanate from the EO to be both "groundbreaking" and "sweeping."

Below we summarize the key provisions of the EO and DOJ's proposed implementation as described in an Advance Notice of Proposed Rulemaking (ANPRM) issued the same day. Interested persons have until April 15, 2024 to comment, and the EO tasks DOJ with issuing a proposed rule by August 26, 2024. No legal restrictions will be operative unless and until a Final Rule is ultimately promulgated.

KEY TAKEAWAYS:

- *The rule is unwritten*. Although DOJ's fact sheet provides a pretty clear (if high-level) idea of where the DOJ intends to go with this authority, its Advance Notice of Proposed Rulemaking (ANPRM) seeks input on 114 different questions (including dozens related to the economic impact of the rule on the market for sensitive personal data and other direct and indirect costs), and in outreach to the private sector, the Biden Administration has signaled a strong desire to receive broad input in order to tailor the rule to avoid unintended consequences.

- *Key areas for comment*. Companies may wish to focus on how their business's transfer of consumer information involving countries of concern—or companies in other locations that are controlled by, for example, covered investors or owners—would be impacted under the ANPRM and its specific examples In particular, companies may wish to focus on the following questions:

- Which “personal identifiers” should be covered by (and excluded from) the rule?
- What data points, use cases, or other information should the Department of Justice consider in determining the bulk thresholds?
- How do businesses use each category of sensitive personal data, particularly in terms of transferring that data outside of the United States, and how would the ranges of bulk threshold under consideration affect business’ ability to engage in transactions with countries of concern or covered persons?
- How would a US party to a data transaction ascertain whether a counterparty to the transaction is a covered person as defined in the ANPRM? What kind of diligence would be necessary?
- What, if any, changes should be made to the definition of “covered person”?
- How easy is it to contract with prospective customers to prevent pass-through sales, re-sale, or onward transfers of bulk US sensitive personal data or government-related data to countries of concern or covered persons?
- Should other types of data transactions (aside from those already contemplated by the ANPRM) be exempt?
- Would general and specific licenses be useful to regulated parties? What about advisory opinions? What would make either process more (or less) useful?
- What new compliance and recordkeeping controls will US persons anticipate needing to comply with the program as described in this ANPRM?

- *Who’s in charge?* DOJ’s Foreign Investment Review Section (FIRS)—the same shop that manages the Department’s work on CFIUS and Team Telecom—will be delegated the authority to implement the EO. FIRS will probably be heavily influenced in its approach to the rulemaking by what it has seen through those processes, and may draw heavily on the concepts and precedents currently implemented on a case-by-case basis in recent mitigation agreements.
- *OFAC is the model*. The regulations issued under this EO will be rooted in IEEPA; violations would carry the potential for civil and criminal penalties. Although the ANPRM forswears a maximalist, strict liability approach, companies will be expected to develop a risk-based compliance regime similar to those implemented to ensure compliance with sanctions regimes. While most companies may not have to comply with due-diligence or affirmative recordkeeping requirements, companies that conduct business in or with countries of concern should be prepared to integrate the final regulations into existing compliance programs.
- Although employment agreements may be considered restricted data transactions, the program will not impact foreign nationals from countries of concern that come to the United States on work or education visas and who may access sensitive personal data while they are in the United States (unless they are specifically designated), because any person located in the United States is not a “covered person” under the ANPRM.

SUMMARY OF THE EO AND ANPRM

Covered Transactions: The EO directs DOJ to identify categories of highly sensitive data transactions between US persons and countries of concern or covered persons that will either be (a) prohibited outright,

or (b) prohibited unless they comply with security requirements (defined by DHS/CISA) that mitigate the risk of access to the data by countries of concern (known as “restricted” transactions).

DOJ’s ANPRM identifies two categories of transactions as the likely subject of rulemaking:

> **Prohibited Data Transactions:** (1) data-brokerage transactions, and (2) genomic-data transactions involving the transfer of bulk human genomic data or biospecimens from which such data can be derived.
>
> **Restricted Data Transactions:** (1) vendor agreements involving the provision of goods and services (including cloud-service agreements); (2) employment agreements (e.g., with a US company’s foreign IT staff located in a country of concern, or with a CEO who otherwise qualifies as a covered person); and (3) investment agreements (those that convey ownership interest or rights and, with it, access to data, akin to what CFIUS currently reviews).
>
> Examples of potential security requirements include data minimization and masking, use of privacy-preserving technologies (e.g., encryption), development of IT systems to prevent unauthorized disclosure, and implementation of logical and physical access controls. The EO prohibits generalized data localization requirements, however.

The ANPRM proposes prohibiting the “knowing” engagement in a prohibited transaction (as opposed to a strict liability standard) to capture persons who knew or should have known the circumstances of the transaction based on their sophistication and the sensitivity of the data (and to exclude liability based on, for example, the unpredictable path that data takes in transiting the Internet, or the employment of covered persons by a foreign company that is not itself covered). The ANPRM also proposes to prohibit US persons from knowingly directing any prohibited transaction (e.g., by their foreign employer) if it would be prohibited if engaged in by a US person.

Covered Data: The ANPRM proposes to regulate transactions involving *either* specific categories of sensitive personal data above certain bulk volume thresholds *or* specific categories of government-related data regardless of volume. The ANPRM contemplates regulating the following categories of **sensitive personal data**, when linked or linkable to an identifiable US person (or group of US persons):

> (1) specifically listed categories and combinations of covered personal identifiers (such as social security numbers and advertising identifiers);
>
> (2) precise geolocation data;
>
> (3) biometric identifiers;
>
> (4) human genomic data;
>
> (5) personal health data; and
>
> (6) personal financial data.

DOJ has proposed ranges of bulk thresholds that vary based on the category of data (some as low as data concerning 101 US persons). This threshold will not apply to transactions involving certain **US Government-related data**, such as precise geolocation data associated with military or other sensitive government functions or sensitive personal data sets explicitly linked to recent former employees, contractors, or officials of the US government.

Countries of Concern: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela.

Covered Persons: The ANPRM defines five categories of covered persons:

> (1) an entity that is 50% or more 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 50% or more 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), and (5);
>
> (4) a foreign person who is primarily resident in the territorial jurisdiction of a country of concern; and
>
> (5) any person (including a US person) designated by the Attorney General as being owned or controlled by or subject to the jurisdiction of a country of concern, or as acting on behalf or purporting to act on behalf of a country of concern or covered person, or knowingly causing or directing a violation of these regulations.

Unless specifically designated under (5), covered persons do not include anyone who is a US citizen, national, or lawful permanent resident; anyone admitted to the United States as a refugee or granted asylum; any entity organized solely under US laws or jurisdiction; and any person located in the United States. Therefore, a Chinese or Russian national located in the United States, or a third country (e.g., an employee) would not be covered unless they are individually designated as such or work for either the country of concern or covered entity.

Exemptions: The EO exempts certain data transactions from the program to the extent that they are:

> (1) considered personal communications or involve information or information materials, as IEEPA uses those terms;
>
> (2) ordinarily incident to and part of financial services, payment processing, or regulatory compliance;
>
> (3) ordinarily incident to and part of ancillary business operations (such as payroll or human resources) within multinational US companies (i.e., between a US person and its subsidiary or affiliate located in a country of concern);
>
> (4) official business or authorized activity of the US Government and its contractors, employees, or grantees (such as federally funded health or research activities, which the funding agencies will regulate themselves); or
>
> (5) transactions required or authorized by federal law or international agreements (such as the exchange of passenger-manifest information, INTERPOL requests, or public health surveillance).

Licensing and Advisory Opinions: The ANPRM considers processes for DOJ to issue general licenses as well as specific licenses to engage in a particular transaction. Entities with licenses may be required to file reports and statements pursuant to their licenses, however, calling to mind the kind of oversight currently undertaken as part of CFIUS mitigation agreements. The ANPRM also contemplates allowing regulated persons to seek advisory opinions on the applicability of the regulations to specific transactions.

Compliance and Enforcement: The ANPRM does not propose to create general due-diligence and recordkeeping requirements; however, failure to do so in some instances may be an aggravating factor in any enforcement action. Reporting may be required for US persons engaging in restricted transactions or licensed transactions. The EO authorizes DOJ to investigate violations of the program and seek civil or criminal penalties under IEEPA.

Other Topics of the EO: In addition to DOJ's forthcoming regulation of sensitive data, the EO directs or encourages these additional steps by other departments and agencies to address data-security risks:

- identifying and mitigating risks arising from prior transfers of bulk sensitive personal data;
- prioritized review by Team Telecom of existing licenses for submarine cable systems with a nexus to countries of concern;
- using grantmaking and contracting authority to ensure federal funds do not support the transfer of sensitive health data and human genomic data to countries of concern;
- further regulating data brokers under the Fair Credit Reporting Act, as previously proposed by the CFPB; and
- studying the risks and benefits of regulating transactions involving types of human 'omic data other than genomic data (e.g., proteomic, epigenomic, and metabolomic data).

AUTHORS

ASSOCIATE

AARON FUTERMAN

WASHINGTON DC +1 202 263 3161

AFUTERMAN@MAYERBROWN.COM

PARTNER

ADAM S. HICKEY

WASHINGTON DC +1 202 263 3024

NEW YORK

AHICKEY@MAYERBROWN.COM

PARTNER

HOWARD W. WALTZMAN

WASHINGTON DC +1 202 263 3848

HWALTZMAN@MAYERBROWN.COM