PAUL HASTINGS

Stay Current

March 2024

Follow @Paul_Hastings

Biden Administration Issues Executive Order and Announces Notice of Proposed Rulemaking Restricting "Countries of Concern" from Accessing Certain U.S. Bulk Sensitive Personal Data and U.S. Government-Related Data

By Scott Flicker, John Gasparini & Ryan Poitras

On February 28, 2024, the Biden Administration issued a new "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the "EO"). The U.S. Department of Justice ("DOJ") concurrently issued a fact sheet ("DOJ Fact Sheet") announcing a forthcoming Advanced Notice of Proposed Rulemaking ("ANPRM") (unofficial version available here) that will provide additional clarity on the scope of the EO and its implementation. The President's action marks a significant expansion of the U.S. Government's authority to prohibit or condition foreign persons' access to U.S. bulk sensitive personal data or U.S. Government-related data and is intended to build upon and supplement other existing authorities, such as case-by-case reviews of transactions by the Committee on Foreign Investment in the United States (CFIUS), Team Telecom, and the Commerce Department under its "ICTS Program." Modeled on existing economic sanctions programs administered by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the new program is expected to impose novel restrictions and additional diligence/compliance requirements on data brokerages and other U.S. businesses dealing in bulk "sensitive personal data" ("SPD") and/or U.S. Government-related data. A summary of the key aspects of the new program follows below:

- **Program Summary**: As contemplated in the EO and DOJ Fact Sheet, the new program will prohibit or impose restrictions on "U.S. person" data transactions involving the transfer of U.S. Bulk SPD or certain U.S. Government-related data to "countries of concern," or to "covered persons" subject to such countries' jurisdiction. DOJ is expected to identify data brokerage transactions and certain genomic-data transactions involving the transfer of data to such jurisdictions and persons as "Prohibited Transactions" due to their inherent sensitivity. Another subset of transactions involving vendor, employment, and investment agreements ("Restricted Transactions") may be permitted subject to compliance with certain predefined security requirements (e.g., organizational cybersecurity posture requirements, physical and logical access controls, data masking and minimization, use of privacy-preserving technologies) to be established by the Cybersecurity and Infrastructure Security Agency within the U.S. Department of Homeland Security to mitigate national security concerns regarding data access by such countries or persons.

Some data transactions are expected to be exempted from the new program, including (i) transactions "ordinarily incident to and part of" financial services, payment processing, and regulatory compliance; (ii) transactions "ordinarily incident to and part of" ancillary business operations within multinational U.S. companies; (iii) activities of the U.S. Government (including contractors, employees, and grantees); and (iv) transactions required or authorized by federal law of international agreements. Purely domestic transactions between U.S. persons are not expected to be within the scope of the new regime. Data transactions involving foreign persons that are not "covered persons" and do not relate to "countries of concern" will generally be permissible on the condition that the foreign person agrees not to resell or give access to such persons or jurisdictions.

- **Persons Subject to the New Program**: The DOJ Fact Sheet contemplates that the ANPRM will identify the following jurisdictions as initial "countries of concern": China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. The EO authorizes the U.S. Attorney General to identify additional jurisdictions as "countries of concern" in consultation with the U.S. State and Commerce Departments.

  "Covered persons" is expected to be defined to include (i) entities owned by, controlled by, or subject to the jurisdiction or direction of a "country of concern" (ii) foreign persons who are employees or contractors of such entities or "countries of concern," and (iii) foreign persons primarily resident in countries of concern." EO also authorizes DOJ to establish a non-exhaustive list of specific entities or individuals designated as "covered persons" subject to the new program.

  "U.S. persons" subject to the new prohibitions and restrictions are expected to include U.S. citizens and lawful permanent residents, persons admitted to the United States as a refugee or granted asylum, entities organized solely under U.S. law or jurisdiction, and persons physically located in the United States. Such persons are expected to fall outside the definition of "covered persons," except to the extent they have been specifically and publicly designated by DOJ as acting on behalf of a "country of concern."

- **Types of Data Subject to the New Program**: The new program will regulate specified categories of data transactions involving "sensitive personal data" that exceed certain bulk volumes. Categories of "sensitive personal data" expected to be covered include (i) certain categories and combinations of "covered personal identifiers" (i.e., a subset of personally-identifiable information to be defined that are reasonably linked to and used to identify an individual), (ii) precise geolocation data, (iii) biometric identifiers, (iv) human genomic data, (v) personal health data, and (vi) personal financial data. Data that is publicly available, personal communications, and expressive information such as videos, art work, or publications will also fall outside the scope of the new program, similar to exemptions available under IEEPA-based OFAC sanctions programs.

  Certain U.S. Government-related data is also expected to be subject to the new regime. "Sensitive personal data" that is linked or linkable to current or recent former U.S. Government employees and contractors (including members of the U.S. military) is expected to be covered, as well as geolocation data that is linked or linkable to certain sensitive U.S. Government locations to be identified on a public list, regardless of the volume of such data provided.

- **Licensing Regime**: The ANPRM is expected to contemplate the establishment of a licensing process. Similar to OFAC sanction programs, DOJ is expected to issue "general licenses" exempting certain data transactions from the scope of the regime. The ANPRM will also likely include a "specific license" regime that will allow transaction parties an opportunity to seek authorization for a transaction that would otherwise be prohibited under the regulations. Parties are also expected to be able to request advisory opinions regarding the application of the regulations to specific transactions. Noncompliance will likely be subject to civil and criminal penalties, and DOJ will likely consider, in any determination of penalty, the adequacy of the U.S. person's compliance program.

Apart from this new regulatory regime, the EO also directs the Departments of Health and Human Services, Defense, and Veterans Affairs to "help ensure that Federal grants, contracts, and awards are not used to facilitate" access to sensitive health data by countries of concern, including "via companies located in the United States." The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (colloquially, "Team Telecom," a DOJ-led, CFIUS-like group of Executive Branch agencies that review foreign investment in U.S. telecommunications companies) will "prioritize review of existing licenses for submarine cable systems" in light of the EO and ANPRM, as well. This is consistent with developments over the past several years that see Team Telecom revisiting previously approved transactions, a departure from its traditional role of exercising authority only in the context of a transfer of control of a business or asset.

DOJ has until August 26, 2024 to issue its proposed regulations implementing the regime. U.S. data brokers and other companies should consider assessing their exposure to the types of "sensitive personal data" that are expected to be subject to the regime, and review their existing customer bases to identify existing customers that may be located or controlled by "countries of concern." As the rules take shape, companies may also want to examine data flows to understand whether any large flows of data to "countries of concern" fit within the anticipated exceptions. While relevant and potentially impactful to any business offshoring personal data from the U.S., these rules may have particular relevance to public companies in the context of broadly increasing scrutiny on public company data privacy and cybersecurity practices in recent years.

Please contact your Paul Hastings representative if you have any questions about the contemplated regime or are interested in submitting public comments to the ANPRM.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact the following Paul Hastings Washington, D.C. lawyers:

Scott M. Flicker
1.202.551.1726
scottflicker@paulhastings.com

John Gasparini
1.202.551.1925
johngasparini@paulhastings.com

Ryan Michael Poitras
1.202.551.1977
ryanpoitras@paulhastings.com