DORSEY
DORSEY+WHITNEY LLP

Justice Proposes to Restrict U.S. Personal Data to Countries of Concern, Including China

by Dave Townsend, Austin T. Chambers, Lawrence Ward, T. Augustine Lo, and Justin T. Huff

The U.S. Department of Justice ("DOJ") released a Notice of Proposed Rulemaking ("Proposed Rule") on October 21 that would prohibit or restrict the transfer of certain data of U.S. persons to China and other countries of concern. Companies involved in cross-border transactions or with operations involving processing of personal data of U.S. persons with any nexus to a country of concern should carefully review the Proposed Rule. The Proposed Rule is intended to regulate transactions involving the transfer of "sensitive" U.S. personal data to countries of concern, but the broad brush of the rule will likely impact companies in numerous industries, including those making cross-border investments, companies involved in technology licensing or services, or entities whose intra-company operations involve the processing of personal U.S. data.

The Proposed Rule would prohibit certain data transfers, while other transfers may occur only if specific security requirements are put in place to protect personal data. These proposed security requirements were published by the Cybersecurity and Infrastructure Security Agency ("CISA") concurrently with the Proposed Rule.

The Proposed Rule implements Executive Order ("EO") 14117 dated February 28, 2024, and builds on the basic framework set out in the earlier Advanced Notice of Proposed Rulemaking ("ANPRM"), as well as comments to the ANPRM.

DOJ has opened a new docket for public comments on the Proposed Rule. Comments are due to DOJ by November 29, 2024.

General Framework and Background

The Proposed Rule outright prohibits certain transactions involving transfers of personal U.S. data to "Countries of Concern" (see definition below), while certain restricted transactions with Countries of Concern are allowed only if an organization implements certain security controls outlined by CISA. Knowing the type of data, the type of transaction, and the location of the recipient or recipients of the data is required to determine whether a prohibition or restriction applies to the proposed transaction or

Related People

- Dave Townsend
- Austin T. Chambers
- Lawrence Ward
- T. Augustine Lo
- Justin T. Huff

Related Capabilities

- National Security Law
- Privacy & Social Media
- Technology Commerce
- China

transfer of the data under the Proposed Rule. We summarize below the types of data and transactions, but generally, the Proposed Rule creates the following two classes of transactions.

- **"Prohibited Transactions."** U.S. persons cannot engage in data brokerage transactions or transactions involving bulk human genomic data or biospecimens from which such data can be ascertained with Countries of Concern.
- **"Restricted Transactions."** Unless the U.S. person adopts CISA's proposed risk mitigation security requirements, U.S. persons cannot engage in the following with Countries of Concern: (1) vendor transactions, (2) employment agreements, and (3) non-passive investment agreements. The CISA security requirements include cybersecurity measures such as basic policies and practices, physical and logical access control, data masking or minimization, encryption, and the use of privacy-protection measures.

Separately, data brokerage transactions with any foreign person would be subject to a requirement that the parties agree to certain conditions, including contractually requiring that foreign persons refrain from reselling or providing access to personal data in a "Country of Concern" or other "Covered Person" (see below for definitions).

U.S. persons also would be prohibited from knowingly facilitating transactions that would otherwise violate the Proposed Rule. These anti-facilitation measures are similar to those imposed under the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") sanctions regulations, which prohibit U.S. persons from directing or referring business opportunities to non-U.S. persons. In addition, the Proposed Rule prohibits evasion of the regulations or causing others to violate them, which could reach non-U.S. person conduct if it induces a U.S. person to assist with a transaction that is prohibited under the Proposed Rule.

The Proposed Rule adopts certain OFAC concepts, such as how a U.S. and non-U.S. person is defined. Like OFAC's regulatory scheme, DOJ can authorize transactions subject to certain conditions, and companies may seek specific licenses from DOJ to engage in an otherwise Restricted Transaction. (As discussed below, the Proposed Rule also contains exemptions for certain classes of transactions, including exemptions for personal communications and information and informational materials that resemble similar provisions under OFAC sanctions regulations.)

The Proposed Rule also establishes certain reporting requirements, but generally does not adopt the approach created under the laws administered by the Committee on Foreign Investment in the United States ("CFIUS"), where companies must determine whether they are required to report certain contemplated transactions or also can voluntarily report a transaction for CFIUS review. DOJ notes that it will coordinate enforcement and administration of the Proposed Rule with CFIUS, especially given that the Proposed Rule covers certain investment transactions by non-U.S. persons in a U.S. business, as described below.

Finally, the Proposed Rule establishes steep civil and criminal penalties for companies and individuals that violate the restrictions or prohibitions. Civil penalties would be up to

$368,136 per violation or two times the transaction value (whichever is greater), and criminal penalties for willful violations would result in fines of up to $1 million dollars and 20 years imprisonment.

Scope of Sensitive U.S. Personal Data

The Proposed Rule prohibits or restricts transactions involving "U.S. Government-Related Data" and certain "Sensitive Personal Data" of U.S. persons (collectively, "Covered Data").

U.S. Government-Related Data includes two types of data:

1. Geolocation data within designed areas – The Proposed Rule identifies sensitive areas by latitude and longitude coordinates, and would cover any precise geolocation coordinates within those areas.
2. Data about U.S. Government personnel marketed as linked to current or recent former U.S. Government employees or contractors – The Proposed Rule defines "recent employees or contractors" as those who worked for the U.S. Government (including the military and intelligence community) within a two-year period preceding a covered transaction.

There is no "bulk" data threshold for U.S. Government-Related Data and thus any quantity of such data is U.S. Government-Related Data, and is Covered Data under the Proposed Rule.

The Proposed Rule defines six categories of "Sensitive Personal Data" of U.S. persons, which would be Covered Data if a transaction involves the processing of such data beyond the specified "bulk" threshold in the preceding twelve months. If a transaction involves the processing of Sensitive Personal Data below the bulk data threshold, the transaction would not be restricted under the Proposed Rule (unless it involves U.S. Government-Related Data). The categories of Sensitive Personal Data and bulk thresholds are as follows:

	Definition	**"Bulk" Threshold (U.S. persons)**
Biometric Identifiers	Physical characteristics that are measurable or behaviors used to recognize or verify the identity of an individual, including facial, voice, retina or iris, palm, fingerprints, gait, or keyboard usage data that are enrolled in a biometric system and the templates used to create such a	1,000

	system.	
Geolocation	Real-time or historical data that identifies the physical location of an individual or a device with a precision of within 1,000 meters	1,000
Human Genomic	Nucleic acid sequences that are the entire set or a subset of genetic instructions found in human cells, including the result of an individual's genetic test and genetic sequencing data.	100
Personal Financial	Data about 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, debts, or trades in a securities portfolio; or data in a credit report or in a consumer report.	10,000
Personal Health	Health information about past, present, or future physical or mental health or conditions of an individual; healthcare information about an individual or payment information about healthcare.	10,000
Personal Identifiers	Identifiers that in combination with any other listed identifier or other data is linked or linkable to sensitive personal data. This includes names linked	100,000

	to device identifiers, social security numbers, driver's license or other government identification numbers, and many others. The definition excludes certain data (e.g., demographic data linked only to other demographic data).	

The Proposed Rule also exempts certain data from Sensitive Personal Data (but not US Government-Related Data), namely data that: (1) does not relate to an individual; (2) is available from public records from a government or widely distributed media; (3) relates to certain personal communications; and (4) meets the definition of informational materials.

Types of Prohibited and Restricted Transactions

The Proposed Rule prohibits or restricts four types of transactions involving Covered Data. Collectively, these four types of transactions are called "Covered Data Transactions."

1. **"Data Brokerage."** Sale of data, licensing of access to data, or other commercial transactions involving the transfer of data from any person to any other person where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.
2. **"Employment Agreements."** Agreements or arrangements where an individual, other than an independent contractor, performs work or job functions in exchange for payment or other consideration, including on a board or committee, executive-level arrangements or services, or employment services at an operational plant.
3. **"Investment Agreements."** The exchange of payment or other consideration for direct or indirect ownership interests or rights in relation to real estate in the United States or a U.S. legal entity. The Proposed Rule excludes from an "Investment Agreement" passive investments such as for publicly traded securities, index funds, or as a limited partner in a venture capital fund.
4. **"Vendor Agreements."** The provision of goods or services, including cloud-computing services, in exchange for payment or other consideration, other than an Employment Agreement.

The Proposed Rule restricts Employment Agreements, Investment Agreements, and Vendor Agreements if they permit "access" by the counterparty to the U.S. Government-Related Data or Sensitive Personal Data. Such transactions are conditionally permitted if the U.S. person implements proposed CISA security requirements (see below). Access is defined broadly to include logical or physical access, the ability to decrypt, view, or to receive Covered Data. Additionally, access may occur where a Covered Person is able to indirectly use or provide others with access to Covered Data (e.g. through technology licenses).

All Covered Data transactions are prohibited outright if they involve "access" to bulk human genomic data or biospecimens from which such data can be ascertained. Data Brokerage transactions with Covered Persons or Countries of Concern are also prohibited outright, absent a separate exemption or DOJ license. Additionally, Data Brokerage transactions with any foreign person are prohibited unless separate conditions are met.

Countries of Concern and Covered Persons

The Proposed Rule prohibits or restricts data transfers to "Countries of Concern" and "Covered Persons." Under the Proposed Rule, Countries of Concern are China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela. The Proposed Rule defines "Covered Persons" as:

1. Non-U.S. entities that are 50 percent or more owned by a Country of Concern;
2. Non-U.S. entities that are 50 percent or more owned by a Covered Person;
3. Non-U.S. employees or contractors of a Country of Concern or entities that are Covered Persons; and
4. Non-U.S. individuals primarily resident in a Country of Concern, and who are not resident in the United States.

In addition to these, DOJ will designate entities and individuals as Covered Persons if they are controlled by or under the jurisdiction of a Country of Concern or a Covered Person, or if they knowingly cause violations of the EO 14117 restrictions.

It is helpful to contrast the definition of a Covered Person with the Proposed Rule definition of a U.S. Person. The Proposed Rule defines a U.S. person as any U.S. citizen, national, or lawful permanent resident, individuals granted refugee or asylee status under U.S. law, an entity organized solely under the laws of the United States, or any person in the United States. A "U.S. Person" is not generally a Covered Person, meaning persons normally resident or actually in the United States, even if employed by (or an affiliate of) an entity based in a County of Concern, would not be a Covered Person. However, DOJ could specifically designate such a person as a Covered Person, as noted above.

The Proposed Rule addresses commenters to the ANPRM who had raised concerns about how to identify Covered Persons, particularly where companies are headquartered in a Country of Concern but operate in third-countries (i.e., not in the United States or a Country of Concern). DOJ responded by adding two examples to the Proposed Rule. One example indicates DOJ's intent that a non-U.S. employee located in a third-country is a Covered Person if they are employed by an entity headquartered in a Country of Concern. The second example is the same, but the employee works for an entity specifically designated by DOJ as a Covered Person, in which case the employee also is a Covered Person. However, the Proposed Rule makes clear that if a person actually is located in the United States, even if they are a citizen of a Country of Concern, the employee is a U.S. person, and not a Covered Person (unless specifically designated as such by DOJ).

Operationally, these distinctions will present difficult compliance questions for companies with ties to China, Russia, or other Covered Persons. Multinational companies will need to carefully assess the Proposed Rule and its various exemptions to determine their compliance obligations, especially where company operations involve cross-border access to data, are located in a Country of Concern, or if any non-U.S. affiliates provide services to the U.S. market.

Requirements for Restricted Transactions

The Proposed Rule permits Restricted Transactions where certain security controls are in place to protect Covered Data. Under CISA's proposed security requirements, these security controls must be implemented with respect to any "Covered System" that is used to process Covered Data as part of a Covered Transaction, regardless of whether Covered Data has been deidentified or encrypted on that system.

The proposed security requirements include both system level and data level security controls. The proposed system and data level controls include numerous security controls common to most information security programs; however several controls impose additional, specific obligations that would require organizations to take additional action to maintain compliance, especially organizations with less mature security programs.

At the system level, organizations would be required to: (1) ensure "basic" organizational cybersecurity policies, procedures and controls are in place; (2) implement strict access controls; and (3) engage in annual risk assessments.

The proposed 'basic' system security policies and procedures would require organizations to: (1) conduct detailed system asset and data inventories; (2) formally designate an individual responsible for cybersecurity risk and governance; (3) remediate vulnerabilities within specified timelines; (4) document and maintain all IT vendor agreements; (5) maintain IT system/network diagrams and maps; (6) implement robust change control procedures; and (7) maintain and review incident response plans.

The proposed system security requirements also include specific requirements regarding management to prevent unauthorized persons from accessing Covered Data. These include strict multi-factor authentication requirements, role-based access controls, strict identity and access management procedures, and detailed logging requirements. The proposed security requirements also include a requirement to engage in detailed annual data and security risk assessments that consider the risks to Covered Data, potential harms to individuals, and develop proposed security controls and mitigations.

At the data level, organizations will be required to implement a mix of controls (established as part of the annual risk assessments) that "fully and effectively" prevent access to data by Covered Persons or Countries of Concern at the data layer. These controls include: (1) data minimization/retention requirements; (2) in transit and at rest encryption requirements (including detailed encryption key management requirements); and (3) the use of privacy enhancing technologies (e.g. homomorphic encryption or

differential privacy techniques).

Each of the proposed security requirements are derived from NIST Cybersecurity Framework and Privacy Framework standards. However, the specificity of these requirements will likely require detailed IT system reviews and the implementation of revised policies and controls to properly secure Covered Data in Covered Transactions.

Exemptions

The Proposed Rule exempts many classes of transactions from the EO 14117 restrictions. In particular, exemptions are proposed for: (1) personal communications that do not transfer anything of value; (2) informational materials involving expressive materials; (3) travel information; (4) U.S. Government activities; (5) financial services; (6) corporate group transactions between a U.S. person and its non-U.S. affiliate if for routine administrative or business activities such as human resources, payroll, taxes, permits, compliance, risk management, travel, and customer support; (7) federal law or international agreement authorized transactions or related transactions; (8) investment agreements that were subject to CFIUS review and certain CFIUS action; (9) telecommunications services transactions if they are ordinarily incident to such services, such as mobile voice and data roaming; (10) drug, biological products, and medical device authorizations if the transactions involve data necessary to obtain or maintain regulatory authorization in a Country of Concern; (11) Clinical investigation and post-marketing surveillance data if the transactions are part of investigations regulated by the Food and Drug Administration ("FDA") or support FDA applications, or pertain to de-identified data needed to support performance, safety, or surveillance of an FDA-authorized item.

Companies will need to review carefully the Proposed Rule definition of these exemptions to see if they mitigate or eliminate compliance burdens as to particular transactions or operations.

Reporting Requirements

The Proposed Rule creates a variety of record keeping and reporting requirements intended to bolster the effectiveness of the prohibitions and restrictions on data transactions. Reporting requirements would apply to U.S. persons if they:

- Reject solicitations to engage in a prohibited data brokerage transaction;
- Know or suspect a non-U.S. person violates the restrictions on resale or transfer to a Country of Concern or Covered Person relating to a Covered Data Transaction;
- Rely on exemptions for drugs, biological products, devices or a combination product in a Country of Concern (see exemptions above);
- Are owned 25% or more by a Country of Concern or Covered Person if they are engaged in Restricted Transactions involving cloud-computing.

Record keeping obligations apply for ten years for U.S. persons that engage in Restricted Transactions that are authorized by the CISA-approved security measures. As a general matter, these would be expected to be kept in a way that an auditor could

easily confirm the U.S. person's compliance with the EO 14117 restrictions and DOJ's Proposed Rule.

Related Law

In discussing the Proposed Rule, DOJ also addresses a newly-enacted law that also regulates data brokerage transactions. Earlier this year, Congress enacted the Protecting Americans' Data from Foreign Adversaries Act ("PADFA"), which restricts transactions of data brokers. PADFA went into effect on June 23, 2024.

Under PADFA, a person meeting the definition of a data broker cannot sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available the personally identifiable sensitive data of a U.S. individual to a foreign adversary or an entity that is controlled by a foreign adversary.

The definition of "personally identifiable sensitive data" under PADFA is defined broadly to include 17 categories of 'sensitive' information that identify a person or that is reasonably linkable to a person or their device. PADFA defines a foreign adversary to mean China, Iran, Russia, or North Korea, and companies domiciled in, headquartered in, with their principal place of business in a foreign adversary, or an entity that is 20 percent owned by an entity or person of a foreign adversary. PADFA defines a "Data Broker" as an entity that makes available, for valuable consideration, data of U.S. individuals that it did not collect directly from such individuals. PADFA excludes from the definition of a Data Broker: (1) entities providing a product or service where "personally identifiable sensitive data, or access to such data, is not the product or service"; and (2) entities that are acting as a service provider.

DOJ identifies several PADFA parameters that are different than the scope of the Proposed Rule. PADFA's reach is limited to those meeting the definition of a Data Broker, while DOJ's Proposed Rule is not limited to data brokers. PADFA has a different definition of what is a foreign adversary than the Proposed Rule's definition of a Country of Concern and a Covered Person. DOJ therefore declined to make any carve-out or exceptions for PADFA but did pledge to implement its EO 14117 authorities in a way that is "harmonized to minimize any conflicting obligations or duplicative enforcement."

Companies will need, therefore, to devote compliance attention to both the EO 14117 restrictions and PADFA to avoid violating U.S. law. Although PADFA is more narrowly tailored in certain respects than the Proposed Rule, PADFA also does not have as many exemptions, and thus may pose an even tougher compliance burden for some companies involved in data-related transactions.

Conclusion

Regardless of industry, companies should consider whether the Proposed Rule or PADFA would restrict their operations or require compliance policies and practices to avoid unlawful activities or miss reporting obligations. Dorsey has attorneys experienced in data privacy and national security matters that can help companies assess the

Proposed Rule and PADFA, and their impacts on businesses. Please contact one of the attorneys below if you have questions.

References and Further Reading:

DOJ Press Release

Fact Sheet

DOJ Proposed Rule

CISA Proposed Security Controls