IAPP **Privacy. Security. Risk. 2025**

Training 28-29 October

Workshops 29 October

Conference 30-31 October

SAN DIEGO

#PSR25

DOJ's Bulk Data Transfer Rule: The Government's Restrictions of Sensitive Data Transfers

Implications and Compliance Considerations

WELCOME AND INTRODUCTIONS

D. Reed Freeman Jr.
Partner, ArentFox Schiff LLP
rfreeman@afslaw.com

Sheila Colclasure
Global Data Integrity and Public Policy Officer, IPG
Sheila.Colclasure@interpublic.com

AGENDA OUTLINE

I. Session Outline

II. Welcome and Introductions

III. Speaker 1 – D. Reed Freedman Jr. (# Mins, Max)
   i. Overview of Bulk Transfer Rule
   ii. What data is covered?
   iii. Who is a “covered person”?
   iv. Exemptions
   v. Does the Rule apply to your company?

IV. Questions and Answers (# Mins, Max)

V. Closing Remarks – (# Mins, Max)

Top-Level, General Summary

- ***Prohibits*** data transactions involving Bulk U.S. Sensitive Personal Data with China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela, and companies or people located there, in connection with "***data brokerage***";
- **Regulates** data brokerage elsewhere; and
- ***Regulates*** such transfers in connection with ***Vendor Agreements, Employment Agreements, and Investment Agreements***.

Overview of the Bulk Data Transfer Rule

On January 8, the DOJ issued a final rule under Executive Order 14117, enforced under the International Emergency Economic Powers Act, which restricts the transfer of sensitive personal and government-related data to certain foreign countries and entities.

DOJ has also issued a:

- press release;
- Compliance Guide;
- FAQs;
- and Implementation and Enforcement Policy.

Overview of the Bulk Data Transfer Rule

What is the main purpose of the rule?

Protect U.S. **national security** by restricting sensitive data transfers to "countries of concern" and "Covered Persons"

When does the rule go into effect?

Took effect on **April 8, 2025**

Civil enforcement of the rule was paused until **July 8, 2025**. Criminal enforcement has not been paused.

Who does the rule apply to?

Applies to **U.S. businesses and individuals** that collect, maintain, or transfer sensitive personal or government-related data.

What Data is Covered?

The Rule restricts the transfer of 2 types of data: Sensitive Personal Data and Government-Related Data

The Rule provides **7 categories of "Sensitive Personal Data"**

1. **Covered personal identifiers** (e.g., name and contact information, financial account numbers, Social Security Numbers, IP addresses, MAC addresses, device IDs, and Ad IDs);
2. **Precise geolocation data** (within 1,000 meters);
3. **Biometric identifiers** (e.g., fingerprints, gait, facial images);
4. **Human 'omic data** (e.g., genomic, epigenomic, proteomic, and transcriptomic data);
5. **Personal health data** (broadly defined);
6. **Personal financial data** (broadly defined); and
7. **Any combination of the above categories**

“Government-Related Data” Transfer and “Countries of Concern”

The DOJ defined “government-related ” as:

1. **Precise geolocation data for any area specifically designated by the Attorney General** as posing a heightened risk of exploitation by a country of concern, which could include military installations, national security, defense or intelligence facilities, or worksites of federal national intelligences personnel and
2. **Any sensitive personal data** that is marketed as **linked or linkable to current or former U.S. government employees** or officials, including from the military or intelligence community.

The Rule does <u>not</u> apply a bulk requirement to transfers of government-related data.

Current list of “Countries of Concern”

China (including Hong Kong and Macau)

Cuba

Iran

North Korea

Russia

Venezuela

This list is subject to change.

“Bulk” Thresholds of Sensitive Data Transfers

Category of “Sensitive Data”	Threshold
1. Covered personal identifiers	**100,000+ U.S. persons**
2. Precise geolocation data	1,000+ U.S. persons
3. Biometric identifiers	1,000+ U.S. persons
4. Human ’omic data	1,000+ U.S. persons
5. Personal health data	**10,000+ U.S. persons**
6. Personal financial data	**10,000+ U.S. persons**
7. Any combinations of the above categories	the lowest number of U.S. persons or U.S. devices in that category of data

- **During a given *12-month period***
- ***Whether through one covered data transaction or multiple covered data transactions involving the same U.S. person and the same foreign person or covered person.***

"Listed Identifiers" Two or More = "Covered Personal Data"

- Full or truncated ***government identification or account number*** (such as a Social Security number, driver's license, passport number, or Alien Registration Number);
- Full ***financial account numbers or PINs*** associated with a financial institution;
- ***Device-based or hardware-based identifier*** (such as IMEI, MAC address, or SIM card number);
- ***Demographic or contact data*** (such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers);
- ***Advertising identifier*** (such as Google Ad ID, Apple ID for Advertisers, or other mobile advertising ID ("MAID"));
- ***Account-authentication data*** (such as account username, account password, or an answer to security questions);
- ***Network-based identifier*** (such as Internet Protocol ("IP") address or cookie data); or
- ***Call-detail data*** (such as Customer Proprietary Network Information ("CPNI")).

Transactions with "Covered Person"

In addition to countries of concern, U.S. companies transferring data to "covered persons" must also comply with the new Rule.

Very generally, entities owned by or incorporated in a country of concern or their employees or others in a country of concern.

The Rule provides **5 categories of "Covered Persons"**

1. **Foreign entities that are 50% or more owned**, individually, or in the aggregate, **by a country of concern** (Includes if principal place of business is in country of concern)
2. **Foreign** individuals who are **employees/contractors of a country of concern**
3. **Foreign individuals who primarily reside in country of concern**
4. **Foreign entities that is 50% or more owned by a covered person** as described in the above parts (1,2, and 3)
5. **Any person designated by the DOJ**/Attorney General

“Covered Transactions”

The DOJ defined “covered transactions” as:

1. Any transaction that involves any access by a country of concern or covered person;
2. To any bulk U.S. sensitive personal data or government-related data that involves 4 types of transactions

A. **Data Brokerages**

Prohibited Transactions
The Rule categorically prohibits high-risk transactions (e.g., data brokerage) involving covered data transactions involving bulk human ‘omic or biospecimen data.

B. **Vendor Agreements**
C. **Employment Agreements**
D. **Investment Agreements**

Restricted Transactions
The Rule permits data transactions from vendor, employment, and investment agreements involving covered data under strict security requirements developed by CISA and record-keeping requirements.

“Covered Transactions” definitions

Data Brokerage

The ***sale of data***, ***licensing of access to data***, or similar commercial transactions

Excluding an employment agreement, investment agreement, or a vendor agreement

Involving the ***transfer of data*** from any person (the provider) to any other person (the recipient)

Where the ***recipient did not collect or process the data*** directly from the individuals linked or linkable to the collected or processed data.

Example 1: Involving a U.S. company selling data to an entity headquartered in a country of concern.

Example 2: Involving an agreement that gives a covered person a license to access government-related data held by the U.S. company.

Example 3: Involving a U.S. company offering annual memberships to persons from a country of concern for a fee that provide members access to U.S. sensitive data.

Examples 4 & 5: Involving the sale of data to a country of concern for advertising purposes.

“Covered Transactions” definitions (cont’d)

Vendor Agreement

“any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.”

- **Example 1:** involving a country of concern vendor that processes and stores bulk precise geolocation data collected through an app owned by a US company
- **Example 2:** involving IT-related services provided by a country of concern vendor to a US medical facility
- **Example 3:** involving a country of concerns’ vendor providing data centers that provide managed services to US companies
- **Example 4:** involving a US mobile games developer that receives software development services from a country of concern vendor

“Covered Transactions” definitions (cont.)

Employment Agreement

“any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level”

- **Example 1:** involving an agreement related to employment of a team of persons.
- **Example 2:** involving the employment of a CEO.
- **Example 3:** involving an agreement to retain a foreign person who primarily resides in a country of concern as project manager to a U.S. company that derives U.S. persons’ biometric identifiers by scraping public photos from social media platforms.
- **Example 4: i**nvolving an arrangement to retain a data scientist.
- **Example 5:** invovling an arrangement to retain a director to the board of directors.

“Covered Transactions” definitions (cont.)

Investment Agreement

any arrangement where a person gains direct or indirect ownership interests or rights in US real estate or a US legal entity in exchange for payment or other consideration and excludes certain passive investments that do not pose national security risks, such as those with less than 10% voting and equity interest without substantive decision-making right

- **Example 1:** A foreign private equity fund located in a country of concern provides capital for the construction of a data center in the U.S. that stores bulk personal health data on U.S. persons in exchange for a majority ownership stake in the data center. The agreement that gives the private equity fund a stake n the data center is an investment agreement.
- **Example 2:** Foreign technology company in a country of concern enters into a shareholders’ agreement with a U.S. business that develops mobile games and social media apps, acquires a minority equity stake in a U.S. business. The shareholder agreement is an investment agreement.

Exemptions

Financial Services

Relates to data transactions that are "ordinarily incident to and part of the provision of financial services."

Activities include, but are not limited to:

1. Banking, capital markets, or financial insurance services;
2. The transfer of covered data **incidental to the purchase and sale of goods and services** (such as online shopping or e-commerce marketplaces);
3. The provision or processing of payments or funds transfers (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, or payment fraud detention); and
4. Provision of investment management services.

Exemptions

Corporate Group Transactions

Relates to data transactions that are "between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control) of a country concern."

Activities include, but are not limited to:

1. **Human resources**;
2. Payroll, and other corporate financial activities.
3. Paying business taxes;
4. Obtaining business permits or licenses;
5. **Sharing data with auditors or law firms for regulatory compliance**;
6. **Risk management**;
7. Business-related travel;
8. **Customer support**;
9. Employee benefits; and
10. Employees' internal and external communications.

Compliance Obligations

The new Data Bulk Transfer Rule enforces both civil and criminal liabilities against violations.

U.S. entities involved in restricted transactions (i.e., covered data transactions in connection with vendor agreements, employment agreements, or investment agreements) are required to

- Establish **risk-based written compliance programs**
- Conduct thorough **due diligence on counterparties**, including ownership and control checks
- **Maintain detailed records**
- Complete annual **independent audits**, and
- **Report** certain transactions and **violations to DOJ.**

Civil Penalties	Up to $368,136 per violation or 2x the transaction value
Criminal Penalties	Up to $1 million in fines and (imprisonment for willful violations)

General Licenses

- General licenses authorize a particular type of transaction for a class of persons without the need to apply for a specific license (i.e., the licenses are self-executing).
- NSD will publish any general licenses on its website and to the Federal Register.
- Can be revoked or modified at the discretion of NSD.

General licenses:

(1) do not excuse compliance with any law or regulation administered by another agency (including **reporting requirements** applicable to the transactions and activities therein licensed),

(2) do not release the licensees or third parties from **civil or criminal liability** for violation of any law or regulation, and

(3) do not constitute a **finding of fact or conclusion of law** with respect to the applicability of any law or regulation.

Specific Licenses

- A written document issued by the NSD to a particular person or entity, authorizing a particular transaction or transactions in response to a license application.
- Presumption of denial for all standard specific license applications.
- Specific licenses are non-transferable and limited to the facts and circumstances in the application.
- May be revoked or modified at any time at the discretion of the NSD.
- Making false or misleading statements in connection with a license application may constitute serious criminal or civil violations.

A specific license:

(1) does not excuse compliance with any law or regulation administered by another Federal agency (including **reporting requirements** applicable to the transactions and activities therein licensed);

(2) does not release the licensees or third parties from **civil or criminal liability for violation of any law or regulation**, and

(3) does not constitute a finding of fact or conclusion of law with respect to the applicability of any law or regulation.

Does the Rule Apply to Your Company?

Your company deals with sensitive data but either does not exceed the bulk thresholds or does not send the data abroad.

- If exporting data, you must ensure not to exceed the "bulk thresholds" and keep adequate records demonstrating that you have not exceeded the thresholds
- Ensure that any vendor, employment, or investment agreements do not bring you within the scope of the Rule (i.e., restricted transactions)

My company collects "covered data" but does not send it to "countries of concern" or "covered persons"

- Ensure that any vendor, employment, or investment agreements do not bring you within the scope of the Rule (i.e., restricted transactions).
- Ensure that you include onward transfer restrictions whenever sending data outside of the U.S.

My company engages in "restricted transactions"

- Your company is sending "covered data" to a "country of concern" under a vendor, employment, or investment agreement.
- You must comply with the robust security requirements developed by the CISA as well as due diligence, audit, recordkeeping, and reporting requirements.

RESOURCE LIST

- ArentFox Schiff Alert: Navigating the DOJ's New Data Transfer Rule: Implications and Compliance Requirements
- Executive Order 14177
- Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons
- Press Release
- Data Security Program: Compliance Guide
- Frequently Asked Questions

Thank you!

D. Reed Freeman Jr.
Partner, ArentFox Schiff LLP
rfreeman@afslaw.com

Sheila Colclasure
Global Data Integrity and Public Policy Officer, IPG
Sheila.Colclasure@interpublic.com

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Privacy. Security. Risk. 2025**
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!