Countdown to Enforcement: Navigating DOJ's Bulk Sensitive Data Access Rule

June 24, 2025

Nancy Libin, Partner, Washington, D.C.

Michael T. Borgia, Partner, Washington, D.C.

Assaf Ariely, Associate, New York City, NY

Davis Wright Tremaine LLP

Today’s Presenters

Nancy Libin

Partner, Washington, D.C.

nancylibin@dwt.com

Michael T. Borgia

Partner, Washington, D.C.

michaelborgia@dwt.com

Assaf Ariely

Associate, New York City, NY

assafariely@dwt.com

Session Overview

- Overview of the DOJ Rule
- Recordkeeping, Reporting, and Compliance Reqs. (effective Oct. 6, 2025)
- DOJ’s Guidance and Limited Enforcement Pause (April 11, 2025)
- (Some) Interpretative and Operational Challenges
  - Access: When does a covered employee or vendor have “access”?
  - Data Brokerage: What do prohibitions mean for third-party advertising?
  - Affiliated Entities: When do employment and vendor restrictions apply?
  - Knowledge: What happens when “knowledge” changes?
  - Corporate Group and Financial Services Exemptions: What is “ordinarily incident”?

Overview of the DOJ Rule

Overview of the DOJ Rule

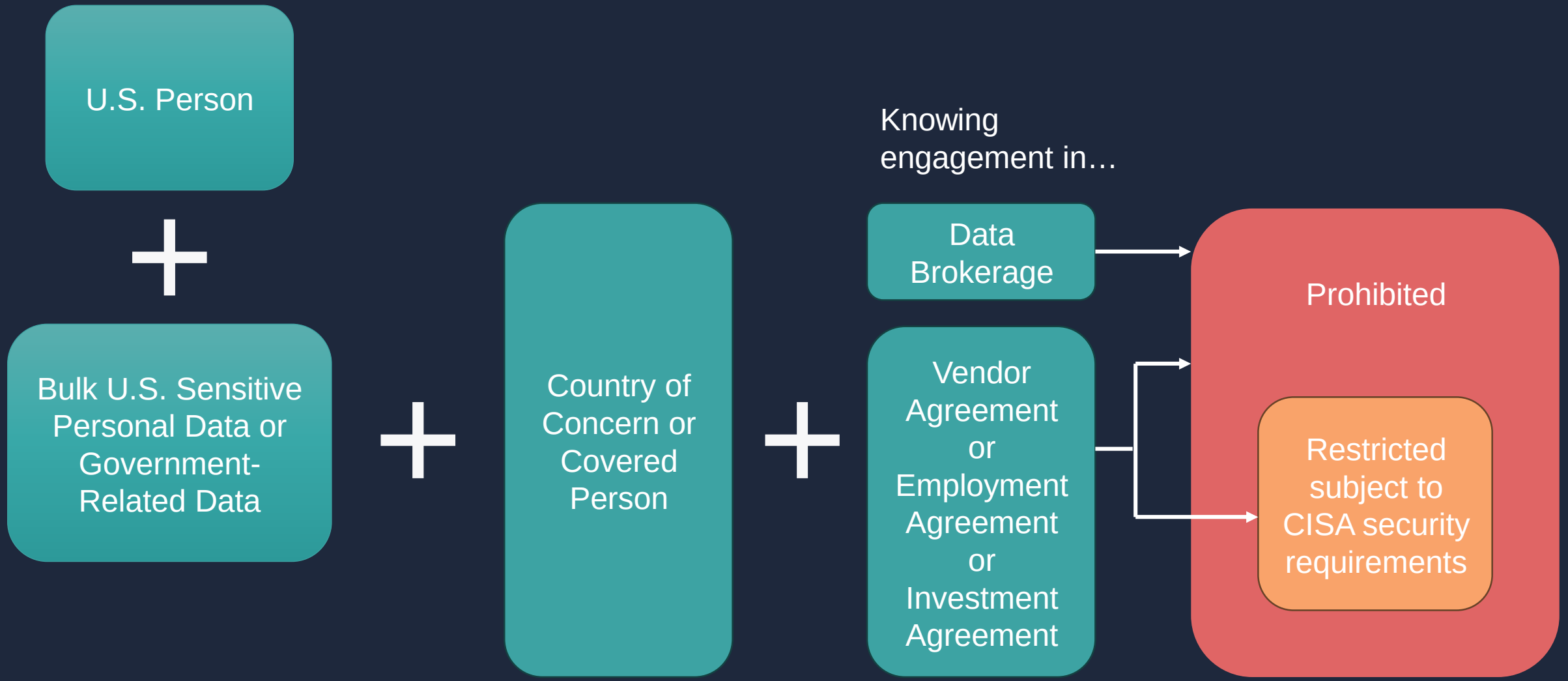
The DOJ Rule restricts or prohibits U.S. persons from knowingly:

1. **Engaging in covered data transactions with a country of concern or covered person, where such transactions involve access by the country of concern or covered person to either government-related data or bulk U.S. sensitive personal data, *OR***
2. **Directing any covered data transaction that would be prohibited or restricted if entered into by a U.S. person**

…Unless an **exemption applies**.

The DOJ Rule also prohibits U.S. persons from engaging in any transaction that "has the purpose of evading, avoiding, causes a violation of, or attempts to violate" the DOJ Rule.

Overview of the DOJ Rule



Overview of the DOJ Rule: Countries of Concern

- China (including Hong Kong and Macau)
- Cuba
- Iran
- North Korea
- Russia
- Venezuela

DOJ has the authority to amend the list of countries via its rulemaking.

Overview of the DOJ Rule: Covered Person

Five classes of covered persons:

1. Foreign entities headquartered in or organized under the laws of a country of concern.
2. Foreign entities 50%+ owned, directly or indirectly, by countries of concern or other covered persons.
3. Foreign persons who are employees or contractors of a country of concern or a covered person.
4. Foreign persons who are primarily resident in a country of concern.
5. Any entity or person designated as a covered person by the Attorney General, based on criteria in the DOJ Rule. Only class that may apply to a U.S. person.

Overview of the DOJ Rule: Covered Data

Bulk U.S. Sensitive Personal Data: a collection or set of **sensitive personal data** relating to U.S. persons, in any format, **regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted**, where such data meets or exceeds the applicable "bulk" thresholds.

Government-Related Data: certain precise geolocation data, regardless of volume, explicitly enumerated in the rule and any sensitive data, regardless of volume, linkable to current or recent employees of the U.S. government.

Overview of the DOJ Rule: Penalties

- ✓ **DOJ will enforce the Rule**
- ✓ **Criminal penalties:** For willful violations, fines up to $1M or imprisonment up to 20 years, or both
- ✓ **Civil penalties:** Up to $368K or twice the value of data transaction, whichever is greater
- ✓ **False statements** may be prosecuted under 18 U.S.C. § 1001

Compliance, Recordkeeping, and Reporting Requirements

Compliance Program Requirements

Due Diligence Requirements (§ 202.1001)

- Verify data flows involved in any restricted transaction
  - Must log the following: (i) types/volumes of covered data, (ii) identity of transacting parties (including ownership, citizenship), (iii) end use of data, and (iv) transfer method
- Verify **identity of vendors** (but not vendors' employees/vendors)
- Written policies **annually certified by an officer, executive, or other employee responsible for compliance**
  - Due diligence
  - CISA requirements
- Other requirements issued by the Attorney General

Audits (§ 202.1002)

- Qualified "independent" annual audit (internal or external) of restricted transactions, including due diligence, recordkeeping, and compliance with CISA requirements
- Audits must be based on "reliable methodology"
- Reports must be retained for **10 years**

Training

- Not required by DOJ Rule but recommended in DOJ guidance

Recordkeeping Requirements

- U.S. persons engaged in covered transactions must "keep a full and accurate record" of each transaction for 10 years (§ 202.1101(a)).
- U.S. persons engaged in any restricted transaction must maintain (§ 202.1101(b)):
  - A written policy describing the person's data compliance program that is certified annually by an officer, executive, or other employee responsible for compliance.
  - A written policy describing implementation of any applicable CISA security requirements that is certified annually by an officer, executive, or other employee responsible for compliance.
  - The results of any annual audits that verify compliance with the CISA security requirements and any conditions on a license.
  - Documentation of required due diligence on data flows for restricted transactions.
  - Documentation of transfer method, dates the transaction began/ended, copies of agreements, copies of documentation received or created in connection with the transaction, and annual certification by an officer, executive, or other employee responsible for compliance of the completeness and accuracy of the records.
- Not applicable to transactions conducted under various exemptions.

Reporting Requirements

- **Ad hoc reports to DOJ** (§ 202.1102)
  - "Every person" must furnish under oath when required by DOJ "complete information relative to any act or transaction or covered data transaction…"
  - Reports may include documents and testimony.
- **Annual Reports** (§ 202.1103)
  - Must be filed by any U.S. person "engaged in a restricted transaction involving cloud-computing services, and that has 25% or more of the U.S. person's equity interests owned … by a country of concern or covered person."
  - Report must include: contact information of U.S. person engaged in transaction, transaction details (data type, volume, transfer method), information about "any persons" participating in the transaction, and copies of "any relevant documentation received or created in connection with the transaction."
- **Reports on Rejected Prohibited Transactions** (§ 202.1104)
  - U.S. persons must file report within 14 days of having received and affirmatively rejected an offer to engage in a prohibited transaction involving data brokerage. Similar content requirements as under § 1103, but must be submitted in accordance with Subpart L (includes certification requirement).

DOJ Guidance and Limited Enforcement Pause

DOJ Guidance: April 11, 2025

DOJ released three key documents:

Implementation and Enforcement Policy: “Limited Enforcement Pause”

Data Security Program: Compliance Guide

Frequently Asked Questions

Press release firmly aligns DOJ Rule to Trump Administration’s priorities, including America First Investment Policy, Iran strategy, and supply chain risks

DOJ's "Limited Enforcement Pause"

- The DOJ Rule became effective on April 8, 2025, but DOJ provided a grace period until **July 8, 2025**.
  - Grace period applies only to civil enforcement.
  - Applies to violations occurring during the grace period.
  - Applies only if company is acting in good faith to get into compliance.

- "Full compliance" expected at the end of the 90-day period.

Compliance Guide and FAQs

- **"Know Your Data":** U.S. persons must understand the type and volume of data they handle, how it's used, and any transactions with covered entities, as ignorance is not a defense; however, **cloud service providers typically aren't required to know their customers' data.**
- **Diligence Obligations:** U.S. persons must screen counterparties to determine they are not covered persons.
  - No obligation to perform diligence on counterparties' employees.
  - U.S. persons are not required to assess "control" of entities by covered persons or countries of concern, but should “exercise caution” in transactions with entities minority owned or controlled by covered persons.
- **No Requirement to Decrypt or Aggregate:** U.S. persons are not required to decrypt or aggregate data to comply with the "know your data" expectations.

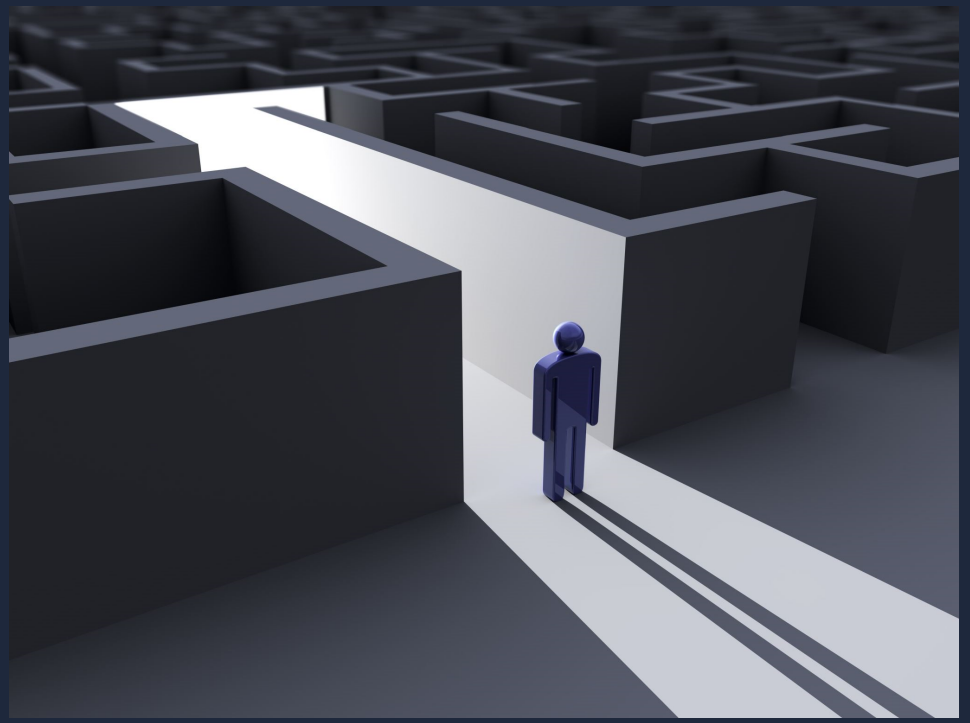
Compliance Guide and FAQs

- **Prohibited Data Brokerage:** Prohibited data brokerage can include U.S. companies with websites or apps using tracking pixels that transfer data to covered persons or countries of concern, expanding beyond traditional data brokerage definitions.
- **Model Contract Language:** The compliance guide provides exemplary language for U.S. persons to restrict data transfers in brokerage transactions with foreign entities, ensuring foreign parties are contractually barred from further data brokerage with covered persons or countries of concern.
  - Customization: Encourages tailoring contract language based on business specifics.
  - Certification: Include language requiring data brokers to certify compliance with the prohibitions on onward sale and evasion.
  - Compliance: Parties must ensure foreign counterparties comply with contractual provisions through risk-based compliance programs.

Compliance Guide and FAQs

- **"Inferences" Generally Are Not Covered Data:** FAQ response says definition of "personal financial data" (a subcategory of "sensitive personal data") does not include "inferences" derived from that data.
  - FAQ response broadly says that the Final Rule restricts only certain categories of transactions involving covered data, "neither of which include inferences on their own."
- **Senior Management Engagement:** Involvement of senior management is crucial for promoting accountability and ensuring compliance.
  - U.S. companies should appoint a compliance leader to integrate controls into daily operations, train employees, and ensure a responsible employee signs annual compliance certifications.

(Some) Interpretive and Operational Challenges



When Does an Employee or Vendor Have "Access"?

- "Access" defined very broadly to include "ability to obtain, read," etc.
  - Access is determined "without regard for the application or effect of" the CISA security requirements.
- If a U.S. person has technical controls in place that would prevent access, but has not fully implemented the CISA security requirements, is there "access"?

Example: A U.S. company maintains covered data. The company has global IT operations, including employing a team of individuals who are citizens of and primarily resident in a country of concern to provide back-end services. The agreements related to employing these individuals are employment agreements. Employment as part of the global IT operations team includes access to the U.S. company's systems containing the covered data. These are prohibited or restricted.

Data Brokerage and Third-Party Advertising

- **Data brokerage** transactions: Any sale of, or licensing of access to, bulk sensitive data where the recipient does not obtain the data directly from the individuals to whom the data pertains. **These transactions are prohibited.**
- Affects any **publisher** that sells ad space and makes personal data of website visitors available or **advertiser** that makes bulk sensitive data available to others in the advertising ecosystem.
  - Covers IP addresses, device IDs, advertising IDs, etc., made available to third-party cookies
  - Requires website publishers and advertisers to obtain contractual commitments even from **foreign persons** who are not covered persons
- Website publishers and advertisers must do the following:
  - Know your vendors (and vendors' vendors)
  - Require third-party tracking technology providers to (1) refrain from engaging in data brokerage transactions, and (2) confirm compliance
  - Report to DOJ any known or suspected violations of this contractual requirement within 14 days of discovery

Affiliated Entities: Employment and Vendor Restrictions

- Covered transactions generally must be between a U.S. person and a covered person or country of concern.
- But what if U.S. person processes covered data through a covered person affiliate, and employees are employed by that affiliate?
  - Vendor relationship?
  - "Knowingly directing"?

Corporate Group Transactions Exemption

- Most requirements do not apply to transactions:
  - (i) Between a U.S. person and its subsidiary or affiliate in a country of concern; and
  - (ii) That are "ordinarily incident to and part of administrative or ancillary business operations."

“Knowledge”: What happens when you learn of a covered transaction?

- "The term knowingly, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result."
- Example: A U.S. service provider offers a software platform for a U.S. company to process sensitive personal data. The provider is unaware of the data specifics and only accesses it for support upon request. The U.S. company, without the provider's knowledge, grants data access to a covered person, in violation of the Final Rule. **The provider hasn't knowingly engaged in a restricted transaction.**
  - But what if the provider receives actual knowledge of the U.S. company’s violation?
  - Or, what if the U.S. company receives actual knowledge that the provider has employees or vendors in countries of concern?

What is “ordinarily incident”?

- Financial Services Exemption
  - “[O]rdinarily incident to and part of the provision of financial services, including”:
    - Banking, capital markets, financial-insurance services
    - Financial activity authorized for national banks by OCC
    - Activities that are “financial in nature or incidental to such financial activity” or “complementary to a financial activity” (~GLBA definition of a financial institutions)
    - Transfers of data “incidental to the purchase and sale of goods and services”
    - Processing of payments or fund transfers
    - Investment management services
- Corporate Group Transactions Exemption
  - “[O]rdinarily incident to and part of administrative or ancillary business operations.”
- Telecommunications Services Exemption
  - “[O]rdinarily incident to and part of the provision of telecommunications services.”

What is “ordinarily incident”?

Why isn’t outsourcing “ordinarily incident”?

Example: A U.S. bank, as ordinarily incident to and part of facilitating payments to U.S. persons in a country of concern, stores and processes the customers' bulk financial data using a data center operated by a third-party service provider in the country of concern. The use of this third-party service provider is a vendor agreement because it involves access by a covered person to personal financial data, but it is an exempt transaction that is ordinarily incident to and part of facilitating international payment.

Example: Same as above, but the underlying payments are between U.S. persons in the United States and do not involve a country of concern. The use of this third-party service provider is a vendor agreement, but it is not an exempt transaction because it involves access by a covered person to bulk personal financial data, and it is not ordinarily incident to facilitating this type of financial activity.

Questions?

Contact Us

Nancy Libin

Partner, Washington, D.C.

nancylibin@dwt.com

Michael T. Borgia

Partner, Washington, D.C.

michaelborgia@dwt.com

Assaf Ariely

Associate, New York City, NY

assafariely@dwt.com