February 10, 2026

DOJ's Regulations on Bulk Sensitive Personal Data and U.S. Government-Related Data

GIBSON DUNN

FTI CONSULTING

Presenters – Gibson Dunn

Vivek Mohan

is a partner in the Palo Alto office of Gibson, Dunn & Crutcher, where he is Co-Chair of the Chambers-ranked Artificial Intelligence practice and a core member of the Privacy, Cybersecurity and Data Innovation practice.

Stephenie Gosnell Handler

is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher, where she advises clients on complex legal, regulatory, and compliance issues relating to international trade, cybersecurity, and technology matters.

Melissa Farrar

is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher, where her practice focuses on white collar defense, internal investigations, and corporate compliance.

Presenters – FTI Consulting

Tracy Wilkison

is a Senior Managing Director with more than 20 years of cybersecurity, national security, litigation and consulting experience. Ms. Wilkison advises clients on their most complicated cybersecurity challenges, from readiness and gap assessments to regulation, enforcement, incident response and complex forensic investigations and litigation.

Elizabeth Kwok

is a Managing Director and highly skilled cybersecurity expert with a distinguished career in fraud investigation and regulatory compliance. Ms. Kwok's extensive experience at the Federal Trade Commission and the Office of the Inspector General, U.S. Department of Commerce has equipped her with a deep understanding of complex financial fraud schemes and emerging cyber threats.

Agenda

01 Background: The U.S. DOJ “Data Security Program”

02 Step-by-Step: Determining Scope

03 Key Issues in Compliance

04 Panelist Roundtable

05 Q&A

06 Appendix: Key Definitions

Background: The U.S. DOJ "Data Security Program"

01

What is the U.S. DOJ Data Security Program?

- The “Data Security Program” (**DSP**) is a term used by the DOJ to describe its expectations for compliance with the “Sensitive Personal Data” regulations issued in December 2024.
  - Regulations issued pursuant to Executive Order 14117, relying on IEEPA (codified at 28 C.F.R. 202).
- The DSP is **unlike any other privacy or cybersecurity regulation**.
  - Includes concepts from privacy, cybersecurity, and export controls.
  - New step and approach for the U.S. - which has generally advocated **free flow of data**.
  - **Unlike** GDPR or other laws focused on “data transfers” - DSP focuses on potential to access.
- Today’s Goals:
  - Understand the DSP.
  - Examine key compliance issues companies face.

Key Dates

- **December 27, 2024:** Regulation finalized
  - (with guidance promised before effective date…)
- **January 8, 2025:** DOJ publishes final rule
- **April 8, 2025:** Regulations effective
- **April 11, 2025:** Guidance issued (*after* effective date)
  - Stated enforcement would not begin for companies taking "good faith efforts to comply" through **July 8, 2025**
- **October 6, 2025:** Certain requirements (due diligence, audit, recordkeeping, annual reports, and rejected transaction reporting) came into effect
- **Today:**
  - Overview of the DSP, discuss certain definitions within the DSP, and examine common issues that companies and stakeholders face with respect to the DSP.

Why the DSP?

"Today, the Justice Department took significant steps to move forward with implementing a critical program to prevent China, Russia, Iran, and other foreign adversaries from using commercial activities to access and exploit U.S. government-related data and Americans' sensitive personal data to … undermine our national security."

- DOJ Press Release, April 11, 2025

Purposes & Countries of Concern

- **Purpose:** Restrict access to covered data by "covered persons," including in "countries of concern."

- **DSP covers two types of data:**
  (1) bulk sensitive personal data of U.S. persons;
  (2) U.S. government-related data.

- A "covered data transaction" involves one of these data types and includes: **(1) data brokerage**; **(2) a vendor agreement**; **(3) an employment agreement**; or **(4) an investment agreement**.

- Such transactions may be prohibited or restricted when "covered persons" from "countries of concern" are involved.

- "**Countries of concern**" are: China (including Hong Kong and Macau), North Korea, Cuba, Russia, Iran, and Venezuela.

Step-by-Step:
Determining Scope

02

Determining Scope

- Understanding how the DSP may impact you requires understanding your exposure:
  - The rule focuses on "**covered data transactions**," which are prohibited unless certain requirements are met.
  - But this also requires understanding if the DSP applies *directly* to you - or whether it is *indirect* - as a vendor or third party.
- The DSP also prohibits any transaction that has the purpose of **evading, avoiding, or otherwise violating the DSP.**

Step 1: How Am I Treated Under the DSP?

- First, ask - are you a "**U.S. person**," or potentially a "**Covered Person**?"
- Different treatment under the DSP based on your status as a:
  - U.S. company
  - Subsidiary/affiliate/parent of U.S. company
  - Vendor to U.S. company
  - Vendor to ex-U.S. company that has U.S. data
  - Ex-U.S. company directly collecting data subject to the DSP

Step 2: What Kind of "Transactions" Are in Scope?

- In-scope transactions are those that involve:
  - **data brokerage**;
  - a **vendor agreement**;
  - an **employment agreement**; or
  - an **investment agreement**.
- Transfers - or the potential for "access" to data between multinationals with subsidiaries in "countries of concern" - not *neatly* addressed, but covered by the DSP.

Step 3: Understanding Data – Potential Covered Data Transactions

- **Covered data transactions** involve the potential for access to:
  - "**government-related data**" or
  - "**bulk U.S. sensitive personal data**"

  by a
  - "**country of concern**" or
  - "**covered person**."
- *Note: To be assessed "without regard" to security measures - including access controls (!)*

Step 4: Exemptions and Compliance – Covered Data Transactions

- Does an exemption under the DSP apply?
  - E.g., limited "corporate group" exception?
- Is it subject to "security requirements" that render access to bulk SPD/U.S. government-related data infeasible by Covered Persons?
  - And, is it then a "restricted transaction" instead of a "prohibited transaction?"
- Is there an applicable license from DOJ permitting the transaction?

And – what are your obligations to third parties if you are not directly subject to the DSP?

Key Exemptions

- **Financial Services** - Data transactions, to the extent that they are ordinarily incident to and part of the provision of financial services
- **Corporate Group Transactions** - Data transactions between a U.S. person and its subsidiary or affiliate located in a country of concern, and **ordinarily incident to and part of administrative or ancillary business operations**
- **Drug/Med Device Regulatory Submissions, Investigations, and Post-Marketing Surveillance** - Data transactions that involve de-identified or pseudonymized sensitive personal data that is required to be submitted to a regulatory entity/covered person to obtain or maintain authorization to research or market a drug, biological product, device, or combination product; as well as those ordinarily incident to and part of: (i) clinical investigations regulated by the U.S. FDA or clinical investigations…or (ii) the collection or processing of clinical care data indicating performance or safety of products, or the collection or processing of post-marketing surveillance data.

Selected Examples

- **Biotechnology** – U.S. genomics firm provides access to sequencing data on more than 100 U.S. individuals to a lab in Hong Kong. Prohibited transaction under § 202.303—covered data transactions involving access by covered person to bulk U.S. human 'omic data are prohibited.

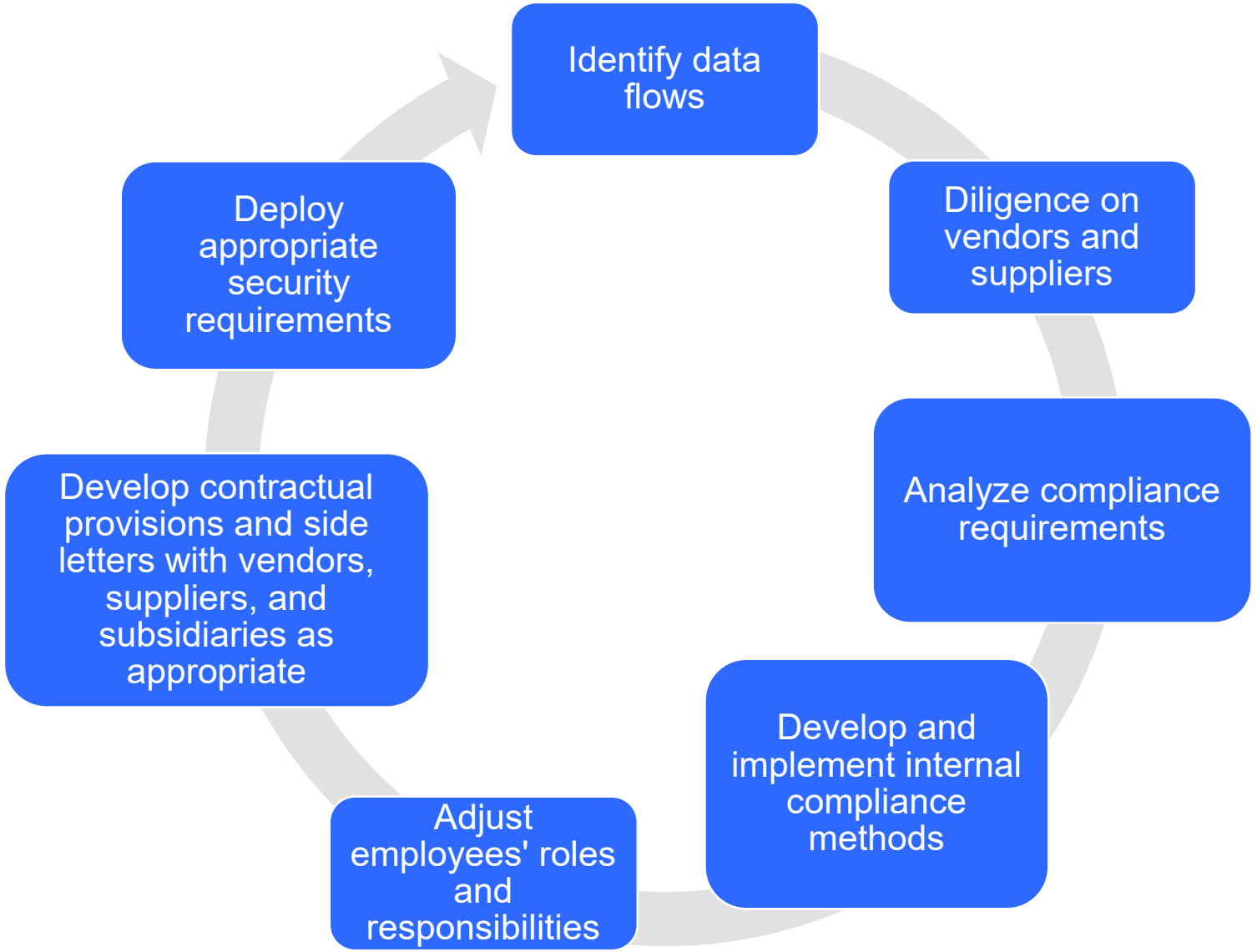
- **Onward Transfer** – U.S. person sells anonymized bulk U.S. financial data to a Singapore entity. U.S. person does not contractually require that the Singapore entity refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a covered person. The transaction is prohibited under § 202.302.

- **Geolocation Data/Government-Related Data** – U.S. person mobile app collects precise geolocation data for ad targeting and provides access to a covered person through a vendor agreement. Some of the collected coordinates fall within the Government-Related Location Data List. The transaction is restricted regardless of the volume of precise geolocation data collected because there is no volume threshold when government-related data is involved. §§ 202.222; 202.401. The transaction may go forward if the U.S. entity complies with the CISA security requirements and all other requirements. §§ 202.248; e.g. 202.1001-02; 202.1101-02.

Key Issues in Compliance

03

What Compliance Looks Like



Key Compliance Issues

- What constitutes sensitive personal data, particularly when considering hardware-based identifiers?

- What is the appropriate level of diligence for a company to conduct on vendors, customers, employees, or affiliates?

Key Compliance Issues (continued)

- What constitutes “access” to covered data?

- When are access controls sufficient to prevent a data transaction from being restricted, and when are they better viewed as “security requirements” that permit a restricted transaction to proceed if implemented correctly?

Key Compliance Issues (continued)

- How to interpret the commonly-misunderstood exemptions - e.g., the “corporate group transaction” exemption and “financial services” exemption?
  - Narrowly tailored – limited to those transactions ordinarily incident to and part of (i) administrative or ancillary business operations between a U.S. company and its non-U.S. subsidiary/affiliate or (ii) the provision of financial services.

Key Compliance Issues (continued)

- The DSP is a complex, broad rule containing inconsistencies and leaving open questions.
- Exemptions are written narrowly.
- No enforcement to date.
- Result is uncertainty about how DSP will be interpreted in practice and what enforcement will look like.
- Companies are taking a wide variety of approaches to compliance—from shutting down certain operations in China and relocating them to the United States to exploring the boundaries of the exemptions.
- Many companies are also deciding not to engage in restricted transactions at all, rather than try to comply with CISA's onerous security requirements.

Litigation Trends

- While no enforcement to date, **some recent plaintiffs' class action lawsuits rely in part on the DSP**.
- The DSP does not provide a private cause of action.
- Plaintiffs bring claims primarily under the Electronic Communications Privacy Act ("ECPA"), which:
  - Prohibits intentionally intercepting wire, oral, or electronic communications or from using the contents of any such communication while knowing that it was illegally intercepted. 18 U.S.C. § 2511(1)(a).
  - Does not apply where one party to the communication has consented to the intercept, **unless intercepted for the purpose of committing any criminal or tortious act in violation of law. 18 U.S.C. § 2511(2)(d).**
- Plaintiffs argue that ECPA's "party exception" does not apply **because defendants' actions were undertaken knowingly and intentionally for the purposes of committing a criminal and tortious act, namely the unlawful transmission of bulk U.S. sensitive personal data to a covered person in violation of the DSP.**

Panelist Roundtable

04

Discussion Questions

1. What's the latest enforcement outlook for the DSP?

2. What's the first thing a company should do if they haven't started compliance yet?

3. How does DSP compare to export controls or sanctions—and what does that mean for governance?

4. What are the most common mistakes/pitfalls/risk areas you're seeing in compliance?

5. Beyond the initial assessment, what does a robust, sustainable compliance program look like? What are the ongoing obligations, such as recordkeeping and audits, that companies need to be prepared for?

6. As a final question, what is the single most important piece of advice each of you would give to an organization trying to demystify this rule and get a handle on its compliance?

Q&A

05

Appendix:
Key Definitions

06

Covered Persons

"**Covered persons**" include:

1) An entity 50% or more owned (directly or indirectly) by, organized/chartered in, or having its principal place of business in, a country of concern;
2) An entity 50% or more owned, directly or indirectly, by a covered person;
3) A foreign person who is an employee or contractor of a country of concern or covered person;
4) A foreign person primarily resident in a country of concern; or
5) Any person specifically designated a covered person by the U.S. Attorney General.

Bulk U.S. Sensitive Personal Data

"**Bulk Sensitive Personal Data**" includes:

1) **Human 'omic** (including info about gene proteins) data on >1,000 U.S. persons (>100 if genomic);

2) **Biometric identifiers** on >1,000 U.S. persons;

3) **Precise geolocation data** on >1,000 U.S. devices;

4) **Personal health data** on >10,000 U.S. persons;

5) **Personal financial data** on >10,000 U.S. persons;

6) **Covered personal identifiers** on >100,000 U.S. persons; or

7) **Combined data**: any collection containing multiple categories meeting the lowest aggregate threshold for any category present.

Covered Data Personal Identifiers

- "**Covered personal identifiers**" is a broad category that covers many types of commonly circulated personal data:
  - (1) Any "listed identifier" **combined with another listed identifier**; or
  - (2) Any listed identifier **combined with other data** enabling it to be linked to other identifiers or other sensitive personal data
- The "**listed identifiers**" defined by the regulations include any piece of data in these categories:
  - **Government identification or account numbers** (e.g., Social Security numbers);
  - **Full financial account numbers or personal identification numbers**;
  - **Device-based or hardware-based identifiers** (e.g., "SIM" card numbers, "IMEI," and "MAC" addresses);
  - **Demographic or contact data** (e.g., name, birth date, or mailing address);
  - **Advertising identifiers** (e.g., Google Advertising ID, Apple ID for Advertisers);
  - **Account-authentication data** (e.g., username or password, answers to security questions);
  - **Network-based identifier** (e.g., IP address, cookie data); or
  - **Call-detail data** (e.g., Customer Proprietary Network Information).

U.S. Government-Related Data

"**Government-Related Data**" includes:

- Any **precise geolocation data, regardless of volume**, for locations on the Government-Related Location Data List (specific geofenced areas associated with military, other government, or sensitive facilities).
- Any **sensitive personal data** (see previous slide), **regardless of volume**, **marketed** as linked to current or recent former U.S. government employees or contractors, including the military and Intelligence Community.

Prohibited Transactions

Prohibited Transactions: Except as authorized pursuant to an exemption or license, U.S. persons cannot knowingly engage in transactions involving “bulk sensitive personal data” or “government-related data” with “covered persons” from “countries of concern” involving:

- **Data-brokerage** (the sale or licensing of data, or similar commercial transactions); or
- **Human genomic data** or human biospecimens from which human genomic data can be derived.

Restricted Transactions

Restricted Transactions: Except as authorized pursuant to an exemption or license, U.S. persons are restricted from knowingly engaging in covered data transactions with a "covered person" or "country of concern" unless controls consistent with **data security requirements** published by the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") are in place.

- Restricted transactions carry **recordkeeping requirements** that are subject to inspection/review by DOJ


Thank You
GIBSON DUNN
FTI CONSULTING