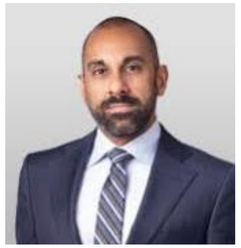
Clark Hill

ACC America
Association of Corporate Counsel

DOJ Bulk Sensitive Data Transfer Rule

Myriah Jaworski
+1 619.819.2447
mjaworski@clarkhill.com



Chirag H. Patel
+1 312.360.2518
cpatel@clarkhill.com

Lionel Bochurberg
+619.819.2442
lbochurberg@clarkhill.com

DSP Overview: A National Security Rule

Bulk Sensitive Data Transfer Rule – a misnomer

- "Data Security Program" – DSP is term used by DOJ to describe its compliance expectations for the Sensitive Personal Data regulations.
  - Biden EO 14117
  - Relies on IEEPA – extraordinary threats
  - DOJ as administrator and enforcer
- Includes national security/export control, privacy and cyber concepts
  - Not first prohibition of data brokerage - PADFAA
- DSP is focused on ***potential to access data.***
  - *Broader application than PADFAA and GDPR regimes*

DPS: IN EFFECT

- **Feb. 2024:** Biden EO
- **Dec. 2024**: Regulations finalized
- **Jan. 8, 2025**: DOJ publishes final rule
- **April 8, 2025**: Regulations effective
  - April 11, 2025: DOJ ***Compliance Guide and FAQs*** issued stating no enforcement for "good efforts to comply" through July 8, 2025
  - **July 8, 2025:** Grace period over, full enforcement.
- **October 6, 2025**: Certain requirements (due diligence, audit, recordkeeping, annual reports, rejected transaction reporting) come into effect.

Who and What is Covered?
(Purpose: regulates **transactions** involving **U.S. Personal Data** and a **COC** or **CP**)

***Countries of concern* are:**


China (including Hong Kong and Macau)


Cuba


Iran


North Korea


Russia


Venezuela

A *covered person* is a **foreign person** who:

- **Foreign person – any foreign entity.**

Becomes CP if:

- **Is 50% or more owned by a Country of Concern;**
- **Is organized or chartered under the laws of a Country of Concern;**
- **Has its primary place of business in a Country of Concern.**
- **Is a employee or contractor of a Country of Concern or covered person; or**
- **Is primarily resident in a Country of Concern.**
- **Is designated by the AG as a COP.**
- **OFAC and Sanctions compliance screening tools can help!**

What types of ***U.S. personal data*** is covered?

- ***U. S. Sensitive Personal Data:*** Six categories, each with "bulk" thresholds:
  - 1) human genomic data on over 100 U.S. persons
  - 2) human 'omic data on over 1,000 U.S. persons
  - 3) biometric identifiers on over 1,000 U.S. persons
  - 4) precise geolocation data on over 1,000 U.S. devices
  - 5) personal health data on over 10,000 U.S. persons
  - 6) personal financial data on over 10,000 U.S. persons
  - 7) certain **covered personal identifiers** (including IP addresses, device IDs, and names and email addresses) for more than 100,000 U.S. persons
  - ***Relevant time period:*** *Rolling 12 month period*
  - ***Includes data that is anonymized, de-id'ed, or encrypted –***
    - National Security, not Privacy law. Threat of bioweapons etc.

What are **Covered Personal Identifiers**?

- ***Combination of 2 or more of the following Listed Identifiers for a U.S. Person (citizen, resident, located in US regardless of citizenship).***
  - Government ID, account numbers (SSNs, passports, drivers license)
  - Full financial account numbers, personal finance IDs
  - Device-based on hardware based IDs (MAC, SIMs)
  - Demographic or contact data (name, DOB, birthplace, zip, address, phone number, email)
  - Advertising IDs – MAIDs
  - Authentication data – usernames and passwords
  - Network based IDs (IP address or cookie data)
  - CPNI

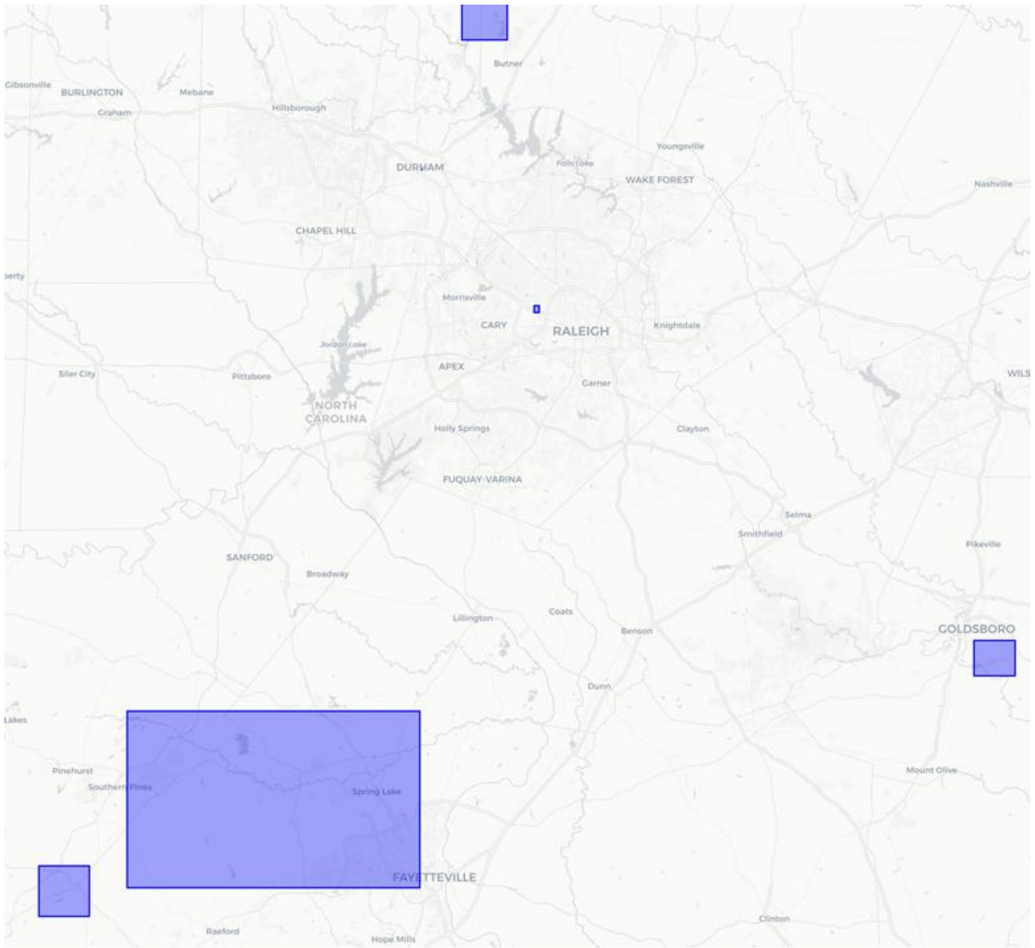
** Adtech is in-scope. Includes data that is anonymized, de-id'ed, or encrypted

What types of Government-related data is covered?

- ***U.S. Government-Related Data:***

  Specific geolocation data and sensitive personal data linked to U.S. government personnel (including contractors and government officials).

  DOJ Rule includes list of geofenced locations – data near government facilities etc.



Covered Data Transactions

- ***Knowingly engage*** – not strict liability, but know *or should have known*.
- The DSP applies when a U.S. person provides a covered person with the ability to access bulk U.S. sensitive personal data or certain U.S. government data and involves one of the following ***transaction*** types:
  - (1) data brokerage,
  - (2) vendor agreement,
  - (3) employment agreement, or
  - (4) investment agreement
- ***Access*** means ability to obtain logical or physical access ***without regard for the application or effect of any security requirements***
- Very broad definition
- Does not require actual access, just the ***ability*** to access.
- Access analysis should be without regard to access controls!

Covered Data Transactions Framework (Prohibited versus Restricted)

Prohibited:

- Data brokerage with covered persons or countries of concern.
- Data brokerage with foreign parties that are not covered persons or countries of concern, unless there are certain onward transfer contractual protections in place.
- ***Access to bulk human 'omic data (including genomic, epigenomic, proteomic or transcriptomic data) or human biospecimens from which bulk human 'omic data can be derived.***

Restricted:

- An employment agreement.
- A vendor agreement, wherein a covered person or a country of concern is providing goods or services to a US person in exchange for compensation.
- An investment agreement.

Covered Data Transactions: Prohibited

- ***Data Brokerage:*** *means the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from one person (provider) to another (the recipient) where the recipient did not collect or process the data directly from individuals linked or linkable to the collected or processed data.*
  - *First and Third Party licensing*
  - *Commercial – Payment or other valuable consideration (IP rights, structured data set, service in exchange for access to data).*
    - *In practice – clarify not commercial?*
  - *Very broad – we don't sell data. But, we license access or provide access as part of a commercial arrangement.*

- ***Onward Transfer Limitations:*** *Any transaction that involves any access to a foreign person, US person must restrict FP from engaging in subsequent data transfer to a CP or COC.*
- What is DOJ doing here? Requiring US companies to regulate/restrict their foreign contracting parties by including onward prohibitions in their contracts.
- So, even if no COC or no CP directly, still need to update your contracts.

Covered Data Transactions: Restricted

- ***Restricted Transactions: Prohibited from knowingly in engaging in:***
  - *Vendor agreement*
  - *Investment agreement*
  - *Employment agreement*
  - ***UNLESS*** *– compliance with Rule's security requirements, due diligence, recordkeeping are met.*
    - *Security requirements may make it impossible/infeasible for the transaction to occur, particularly in the vendor and investment context.*

- ***Vendor –*** *goods or services.*
- ***Employment –*** *includes board membership even if not paid. (Not as relevant because most foreign employees are employed through affiliates or CPs).*
- **Investment:**
  - **Excludes passive investments in theory.**
  - **But, if foreign entity has access (assumed) then it becomes active in-scope investment and a RT.**
  - *In these contexts, will need to put security limitations around the individual's access to covered data.*
  - **DOJ Final Rule has illustrative examples.**

Compliance: Specific Security Requirements

- ***Restrict transactions are prohibited <u>unless</u> business meets Specific Requirements***
  - Security requirements stem from Cybersecurity Information Sharing Act of 2015 (CISA 2015)
  - Check No prohibited transactions
  - Establish a security program including security measures with respect to restrict transactions
    - Note Broad language in Bulk Rules FAQ:" ***must "fully and effectively" prevent access"***
  - Comply with contractual obligations for onward transfers to any foreign person

Compliance Requirements

- ***Meet Specific Requirements***
  - No prohibited transactions
  - Establish security measures with respect to restrict transactions
  - Comply with contractual obligations for onward transfers to any foreign person
- ***Implement Security Program – must "fully and effectively" prevent access***
  - Internal compliance controls – data minimization, access and key management
  - Employee roles
  - Contractual language and vendor diligence
- **Annual Audits**
- **Reports** – notify DOJ of any unlawful transfers offers; annual report if engaged in certain data transfers
- **Recordkeeping** – 10 years

Exemptions & Licenses

- ***Exemptions are misunderstood***
  - 11 total exemptions
  - Corporate Group Transaction
  - Financial services – ordinarily incident to the provision of financial services
  - De-identified or pseudonymized data for drug/med device submissions

- ***DOJ can issue licenses –*** *general (for classes of transactions) or specific (to company); may have conditions and issued rarely.*
- **DOJ Advisory opinions – regulated parties can seek**
- ***DOJ/AG can add additional COCS and CPs***

Illustrative Scenarios

- Adtech partnerships
- Investment from a Hong Kong-based investment fund
- Use of engineering/development talent in China
- Life sciences partnering / licensing
- Access to corporate resources by affiliate entities/offices in China

Federal Enforcement

- Enforced by DOJ and Commerce Department (enforcement began July 9, 2025)
- Civil monetary fines of up to $368,136 per violation or twice the value of the transaction, whichever is greater.
- Criminal penalties of up to $1,000,000 or 20-years' imprisonment for willful violations.
- Actual knowledge or reason to know
- What has DOJ signaled re: enforcement?
  - Relatively new, but staffing up
  - Signaled enforcement focus – compliance guide and FAQs
  - Voluntary self disclosure program comparable to OFAC

Litigation Trends

- DSP does not have a private right of action

- Recent class action lawsuits rely on alleged DSP rule violations
  - Targeting adtech and retailers
  - To show "crime/fraud" for ECPA party exception not to apply
  - Similar to HIPAA violation allegations in ECPA actions against healthcare entities

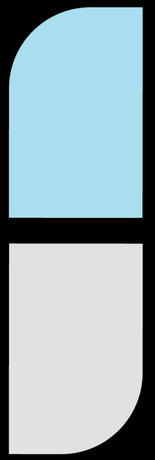
Litigation Trends

- ***Christy v. Lenovo (United States) Inc.*** **(N.D. Cal.)**
  - Claims under CIPA, ECPA, UCL, CDAFA, and Common Law. Alleges conduct is both a privacy harm and a national security risk under the Bulk Sensitive Data Transfer Rule
  - ECPA has a party exception to liability (intercepting own conversation is not violation). "Party exception" does not apply if interception was to commit a criminal or tortious act.
  - Claims Lenovo integrated tracking from major ad-tech and analytics vendors (including TikTok, Meta/Facebook, Microsoft, Google, Adobe, Index Exchange, Snap, and others)
  - Alleges Lenovo collected or maintained data relating to more than 100,000 U.S. persons, meeting the regulation's "bulk" threshold for covered personal identifiers, and then transmitted or made that data accessible to "covered persons," including Lenovo Group entities tied to China
  - Defines a nationwide class of U.S. users whose electronic communications with Lenovo's website were allegedly intercepted and used on or after April 8, 2025 (also defines California subclasses)

Potential Compliance Approach

- **Bulk Data Rule Scope Assessments**
  - Create customer screening process to determine foreign and covered persons who receive data
  - Identify high risk systems
  - Analyze which employee and vendors have access to high risk systems
- **Remediate Non-Compliant Transactions**
- Develop Compliance Program
  - Diligence
  - Record Keeping
  - Reporting

Questions?



Clark Hill

Thank You

Legal Disclaimer
The views and opinions expressed in this material represent the view of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this presentation constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

Clark Hill