CROSS-BORDER DATA FORUM

“PERSONAL DATA AS A DUAL-USE TECHNOLOGY: PRIVACY PROFESSIONALS FACE NEW EXPORT CONTROLS”

IAPP Webinar

February 19, 2026

CBDF
CROSS-BORDER DATA FORUM

Overview

- Big picture on U.S. data policy toward China and other countries of concern
- Key definitions under the DOJ Bulk Data Rule and Protecting Americans' Data from Foreign Adversary Act (PADFA)
- Some implications of those definitions
- Five practical tips for privacy professionals

National Security, Data, and Other New Laws

- The intuition: **risky to national security** if adversary nations have access to sensitive data of Americans
  - Duke data broker study – data brokers sell **precise geolocation data** to track military and other personnel for a few cents/person
  - If you were a member of Congress – **comfortable if adversary nations can track U.S. military personnel?**
  - Sensitive data to adversary nations:
    - **Intelligence** advantages – they learn about U.S.
      - No similar U.S. visibility about Russia/China individuals
    - **Counter-intelligence** advantages – they learn about U.S. actions such as U.S. spies
    - **Influence operations** – blackmail, disinformation, etc. using the data

Another Theme on National Security and Data: AI

- **Great power competition and artificial intelligence**
  - Chinese advantages include:
    - Access to data on large population
    - Government scope to mandate data into datasets
  - U.S. advantages include:
    - Commercial AI success and leadership
    - Cloud infrastructure to scale AI
- **A national security lens**
  - **Personal data as strategic asset for great power competition**
    - How would the government like to have a specialized adversary database about actions of US individuals?
  - **Should data be retained within the U.S.? For online advertising and social networks?**

CBDF
CROSS-BORDER DATA FORUM

Recent U.S. Legal Responses to China

- Numerous initiatives: cranes in ports; software in electric cars
- **EO 14117 to limit bulk data sales** to foreign adversaries (2/24)
  - Swire/Sacks, "Limiting Data Broker Sales in the Name of U.S. National Security: Questions on Substance and Messaging" (Lawfare Feb 2024)
  - **DOJ Bulk Data Rule is now in effect**, for enforcement, criminal and civil penalties
- New law: **Protecting Americans' Data From Foreign Adversaries Act (PADFA)** (4/24)
  - Passed 500-0 in House, never got a mark-up in either chamber; same bill as TikTok ban
  - Swire, "White Paper on Clarifying Definitions in the Protecting Americans' Data from Foreign Adversaries Act of 2024" (May 2024)
  - Definitions broad:
    - Apply to **sensitive data of one U.S. individual** to China
    - Apply to **first-party data** about website use, beyond state "sensitive data" definitions
  - Enforced by FTC – new enforcement letter (Nigel Cory will discuss)

CBDF
CROSS-BORDER DATA FORUM

“Dual Use” Technologies, Data, and Social Media

- **“Dual use” technologies – both military & civilian uses**
  - Historically, fighter jet technology
  - Today, treat personal data online as a dual use technology?
- If so, potentially broad limits on transfers of personal data to China and other countries
  - Zweiful-Keegan: **“The beginning of the end of the free flow of data”**
  - **Regulation of data for national security purposes, not protecting individual rights**
- Swire & Sacks writing
  - Personal Data as a Dual-Use Technology: Critically Assessing the New Alliance of Privacy and National Security (at SSRN.com now; forthcoming **Virginia Journal of International Law**)
  - “**Personal Data as a Dual-Use Technology, Privacy Professionals Face New Export Controls**”, **IAPP** 11/25

Questions for the Emerging National Security Consensus

- **Will the rules be effective**, to block data flows to China and other adversaries?
  - Good idea to create a **U.S. "National Security Firewall",** analogous to Great Firewall of China?
  - Good idea for U.S. to abandon its previous policy of "**free flow of data** on the Internet"?
- Will these rules succeed as a **sanctions regime**?
  - Sanctions regimes tend to work better to address acute harms, for short period
  - Over time, evasion of sanctions often succeeds
- How do national security risks compare to **national security advantages of U.S. engagement with the world?**
  - If U.S. rules apply to **onward transfer** through other countries, what happens when data transfers to Latin America, Africa, and rest of the world?
  - Soft power and other national security advantages from continued engagement
  - **Advantages from engagement/entanglement** – Trump administration has approved NVIDIA chips to China, to encourage China's dependency on US technology

DOJ Bulk Data Rule: Countries of Concern

- China
- Russia
- North Korea
- Iran
- Cuba
- Venezuela

Bulk Data Rule: Broad Definition of "Covered Persons"

- **Prohibited transactions with "covered persons"**
- Does **not apply to "U.S. persons"**
- **Broad definition of entities** owned or controlled by countries of concern:

(1) foreign entities that are 50 percent or more owned by a country of concern, organized under the laws of a country of concern, or has its principal place of business in a country of concern;

(2) foreign entities that are 50 percent or more owned by a covered person;

(3) **foreign employees** or contractors of countries of concern or entities that are covered persons;

(4) foreign individuals **primarily resident in countries of concern.**

- Also, anyone on a prohibited "entities" list

Broad Definition of "Covered data transaction"

- *"A covered data transaction* is any *transaction* that involves any bulk U.S. sensitive personal data or government-related data and that involves: **(1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement**."
- **Ban on "data brokerage"**
  - Definitions of "bulk" vary by category of sensitive data
  - Target any sales (access more generally) of U.S. military or U.S. federal employee data
- Broad scope of **vendor/employment/investment agreements**
  - These would be subject to **new data security rules**, not outright ban

Broad definition of “data brokerage”

- “The program would define *data brokerage* as the sale of, licensing of *access* to, or similar commercial *transactions* 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.”**

Easy to Exceed the Minimums for "Bulk Data"

- Precise **geolocation** data (1000 devices)
- Biometric data (1000)
- Genomic (and other 'omic) data (100)
- Personal health data (10,000)
- Personal financial data (10,000)
- Certain personal identifiers (somewhat narrower than PII) (100,000)
- Note: Rule applies **"regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted"**
  - Rationale – protect against advanced persistent threats – countries of concern

CBDF
CROSS-BORDER DATA FORUM

Some policy themes on the big picture

- We are **early days** in understanding the intersection of data and national security
- Possible **political alliance for national security and privacy**
  - "Protect national security" – often easier to pass the laws; PADFA passed unanimously
  - "Regulate the free market" – often, more difficult to pass laws
- **The Trump administration**
  - Biden largely continued earlier Trump China initiatives
  - **So far, Trump has largely continued Biden's China initiatives**
    - The Bulk Data Rule and PADFA are moving forward
      - However, turnover of senior civil servants in DOJ National Security Division, which wrote the Bulk Data Rule
  - Potentially, data will be part of a Trump/Xi "**grand bargain**", and data flows will ease
  - Potentially, **greater U.S. decoupling with China**, presumably with additional new data limits

CBDF
CROSS-BORDER DATA FORUM

Some themes for privacy professionals

1. Consider how to bring **national security expertise** to the team that has led the company's privacy compliance.
2. Benefit from **synergies** in complying for privacy and national security purposes.
3. Coordinate compliance with the **cybersecurity team**.
    1. Many DOJ covered transactions permit transfers while require strong cybersecurity, for: vendor, employment, and investment agreements
4. **Monitor how the new definitions** are interpreted.
5. Finally, consider how these national security issues fit into your company's **overall data governance structure.**

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ76ul

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: **livewebconteam@iapp.org**