

# Future-Proofing Privacy Programs: Lessons from PADFAA and the Bulk Data Access Rule

**Elena Vekilov**  
NielsenIQ

**Joseph Emerson**  
Protiviti

**Aaron Burstein**  
Kelley Drye & Warren

November 12, 2025

# Our Agenda

1. Review key requirements of the Rule and PADFA
2. Discuss how compliance can build on privacy program elements
3. Discuss how Rule/PADFA compliance can reinforce privacy programs
4. Answer your questions

# Background on Bulk Data Rule and PADFA



## PADFA

- 15 U.S.C. § 9901
- Prohibits “**data brokers**” from selling “personally identifiable sensitive information” to “foreign adversary countries” or entities they control
- “Data broker”: sells U.S. personal data that was not directly collected from individuals to third parties
- “Sensitive” data includes health, financial account, biometric, genetic, precise geo, private communications
- “Control” is determined by direct or indirect ownership – U.S.-based entities are in scope
- Enforced by FTC
- Civil penalties of up to \$53,088 per violation

## Bulk Data Rule

- 28 C.F.R. part 202
- Issued by DOJ under IEEPA
- Prohibits “**data brokerage**” and restricts access to U.S. bulk sensitive personal data through **employment**, **vendor**, or **investment** agreements by countries of concern or “covered persons”
- “Data brokerage” includes the sale of data collected on a **first-party basis**
- “Sensitive” data includes combinations of online identifiers as well as the sensitive categories under PADFA
- “Control” is determined by direct or indirect control but U.S.-based entities generally are not covered persons

**Both regulations are currently enforceable.**

# Key Takeaways

- The scope of PADFA is different from the scope of the Bulk Data Rule.
- The Rule has a **much** broader definition of “data broker,” which includes sales of first-party data.
- The Rule’s ownership test has brighter lines but applies to a much broader range of activities: employment, vendor, and investment agreements in addition to data brokerage.

# Guiding Questions for Rule/PADFA Compliance



- How do you do an initial assessment of exposure?
- Which elements of a privacy program are helpful in assessing exposure?  
What if you're starting from scratch?
- Which teams should be part of the assessment and compliance process?
- Is Rule/PADFA compliance a ***privacy team*** responsibility? How can this team communicate the importance of compliance?

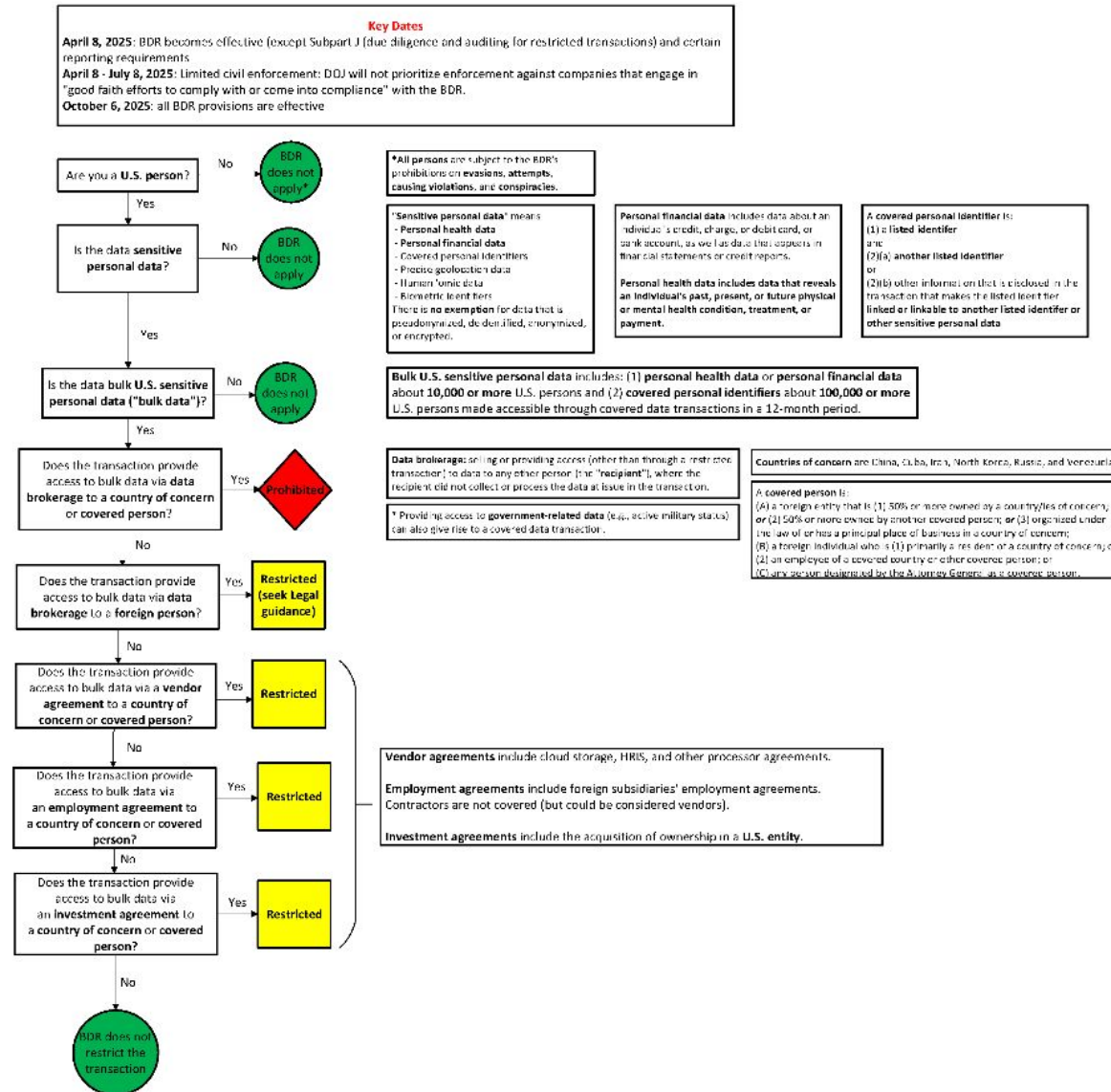
# Guiding Questions for Mitigation

- What is the Data Security Program? Is it mandatory?
- What are the options to remedy prohibitions on data brokerage?
- How can companies control risks of restricted agreements under the Bulk Data Rule?

PADFA/Rule compliance efforts can help strengthen:

- Data mapping
- Auditing capabilities
- Tracking technology management processes
- Customer and supplier due diligence processes

# Bulk Data Rule – High-Level Decision Tree





## Elena Vekilov

CPO & Global General Counsel, Data Security, Product, & AI  
NielsenIQ

## Joseph Emerson

Managing Director  
Protiviti

## Aaron Burstein

Partner  
Kelley Drye & Warren LLP