AN A.S. PRATT PUBLICATION
SEPTEMBER 2025
VOL. 11 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 7** **September 2025**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Data Privacy Implications of DOJ Bulk Sensitive Personal Data Rule Under Executive Order 14117 as Seen Through the Lens of Vendor Contracting and International Norms

By Frederick C. Bingham, Jeewon K. Serrato and Shruti Bhutani Arora*

This article examines the regulatory, contractual, and compliance implications of Executive Order 14117 and the accompanying Department of Justice (DOJ) rule, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern. Specifically, it analyzes the DOJ's expansive definition of sensitive personal data and its significant decision to treat anonymized, de-identified, and pseudonymized data as within regulatory scope – a stark contrast to consumer privacy statutes such as the California Consumer Privacy Act (CCPA), which generally exclude such data from coverage. Through a U.S.-centric but internationally informed lens, this article explores the due diligence obligations imposed on businesses, including contractual requirements that emerge from these rules. Further, a comparative review of global standards (e.g., GDPR) highlights tensions in defining "anonymized" data and the practical impact of the requirement of rendering data fully immune to re-identification. Ethical considerations and constitutional questions surrounding national security-based data restrictions are also addressed.

EXECUTIVE ORDER 14117 AND RULEMAKING BACKGROUND

Overview of EO 14117

Executive Order 14117 of February 28, 2024 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern) mandates U.S. Department of Justice to restrict access by "countries of concern" to Americans' "bulk sensitive personal data" and U.S. government-related data.[1] The order defines "sensitive personal data" expansively – including personal

* Frederick C. Bingham, a lawyer with Kasowitz LLP, specializes in data privacy, cybersecurity, and artificial intelligence. Jeewon K. Serrato leads Pillsbury Winthrop Shaw Pittman LLP's Consumer Protection team, co-leads the firm's Retail Industry team, and is a leader in the firm's Global AI Task Force. Shruti Bhutani Arora is a partner in Pillsbury's San Francisco office who specializes in privacy compliance and complex technology transactions.

[1] Exec. Order No. 14,117, 89 Fed. Reg. 15,421 (Mar. 1, 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

identifiers, geolocation data, biometrics, genomic and other "human 'omic" data, health data, and financial data, whenever linkable to U.S. individuals. EO 14117 invokes the International Emergency Economic Powers Act (IEEPA) authority and directs the Attorney General to promulgate regulations (the Data Security Program) implementing these restrictions.

Rulemaking Timeline

DOJ's National Security Division (NSD) issued an Advance Notice of Proposed Rulemaking (ANPRM) concurrently with EO 14117 (Feb. 2024),[2] soliciting comments on scope (comments closed Apr. 19, 2024). It followed with a full Notice of Proposed Rulemaking (NPRM) on Oct. 18, 2024,[3] providing draft regulations for public comment (closing Nov. 29, 2024). The final rule was published Jan. 8, 2025 (codified at 28 C.F.R. Part 202, 90 FR 1706),[4] with an effective date in Spring 2025. These documents (ANPRM, NPRM, Final Rule) are the primary sources for the program's substantive requirements, although the DOJ has also released an initial FAQ addressing 100 questions regarding scope, compliance, and obligations.[5]

Compliance Deadline

The DSP went into effect on April 8, 2025, but some requirements were delayed. The compliance requirements, including affirmative due diligence, become effective on October 6, 2025. The final rule applies prospectively to transactions occurring on or after its effective date (April 8, 2025), even if the underlying agreements existed before the rule; therefore, continued access to sensitive data under current vendor, employment, and commercial relationships must comply with the rule.

DATA PRIVACY COMPLIANCE IMPLICATIONS

Scope of Coverage

The rule (28 C.F.R. Part 202) prohibits U.S. persons from engaging in transactions involving "bulk U.S. sensitive personal data" or U.S. government-related data with

---

[2] U.S. Dep't of Justice, Nat'l Sec. Div., Data Security, https://www.justice.gov/nsd/data-security#:~:text=Advance%20Notice%20of%20Proposed%20Rulemaking,closed%20on%20April%2019%2C%202024 (last visited June 16, 2025).

[3] Id. at "Notice of Proposed Rulemaking and Proposed Security Requirements . . . public comment period for the NPRM closed on November 29, 2024."

[4] 28 C.F.R. pt. 202 (2025), https://www.ecfr.gov/current/title-28/chapter-I/part-202 (last visited June 16, 2025).

[5] U.S. Dep't of Justice, Nat'l Sec. Div., Data Security Program: FAQs 1 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396351/dl (last visited June 16, 2025).

countries of concern or covered persons. "Bulk" is defined by quantitative thresholds varying by data type and is applied to datasets, not individual records.[6] In effect, any large-scale transfer or sale of the listed personal data categories to foreign adversaries may be restricted. Compliance thus would require identifying whether a dataset meets the threshold for coverage.

Non-Public Data

The EO and rule target non-public data. Sensitive personal data is already narrowly defined and the rule explicitly excludes publicly available information (e.g., publicly filed court records). For compliance, entities should distinguish between public and covered data sources. In addition, the rule excludes "trade secret" (as defined in 18 U.S.C. § 1839(3)) or "proprietary information" (as defined in 50 U.S.C. § 1708(d)(7)).[7]

Aggregated and Anonymized Data

Notably, the rule includes aggregated or supposedly "anonymized" data in its scope: DOJ declined requests to exempt anonymized or de-identified data, reasoning that even aggregated anonymized datasets can be re-identified by adversaries.[8]

Compliance Program Requirements

Covered entities will need robust compliance and data governance policies in place. This includes establishing policies to identify covered data, screening transactions by volume and by counterparty (e.g., countries of concern), and implementing transaction controls (e.g., blocking prohibited transfers). The rule's broad scope means many entities (data brokers, health systems, online platforms, cloud providers, etc.) must assess operations to ensure no "bulk" data flows are made to disallowed parties. DOJ's rulemaking materials indicate companies must err on the side of caution; for example, commenters warned that excluding "de-identified" data would undermine national security goals, so DOJ kept the broader definition.[9] Companies should assess whether existing data loss prevention tools can be leveraged to identify the data transactions that may be in scope and to apply the new data flow restrictions.

---

[6] 90 Fed. Reg. 1636, 1644 (Jan. 8, 2025) (commentary at 12 pertaining to § 202.206), https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern (last visited June 16, 2025).

[7] 28 C.F.R. § 202.249(a)(1) (2025).

[8] Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern, 90 Fed. Reg. 30,804, 63 (May 8, 2025), https://www.justice.gov/nsd/media/1382521/dl (last visited June 16, 2025).

[9] Id. at 106.

DUE DILIGENCE AND OPERATIONALIZATION

Due Diligence Obligations

Subpart J of the final rule (§202.1001) requires U.S. persons to conduct "sufficient due diligence" before engaging in any potentially covered transaction. While DOJ declined to mandate rigid procedures, it makes clear that entities must be able to assess ownership and control of data and parties involved.[10] In practice, this means verifying counterparty nationalities, ownership (e.g., foreign investments or affiliations) and the nature of the data handled. Covered transactions trigger further compliance steps (reporting to DOJ, recordkeeping under §202.1100s, and possibly seeking an exemption or license). Potential checklist of due diligence steps may include:

- *Data Identification and Classification*: Determine whether any data collected or shared meets the rule's definitions for U.S. government-related data or bulk U.S. sensitive personal data.
- *Transaction Assessment*: Review whether any transaction involves the transfer, provision of access, licensing, or other forms of data sharing covered by the rule.
- *Volume Thresholds*: Evaluate if the volume of data involved in a transaction meets or exceeds regulatory thresholds for categories like health, geolocation, biometric, or financial data.
- *Recipient Evaluation*: Screen transaction counterparties to assess whether they are located in or subject to the jurisdiction of countries of concern, or are owned or controlled by covered persons.
- *Purpose and Risk Analysis*: Assess the end use of the data and determine whether it could create a national security risk, including whether anonymized or de-identified data could be re-identified.
- *Internal Governance and Records*: Maintain written internal procedures to assess covered data transactions and document risk evaluations and compliance efforts and create/retain *auditabl*e logs.

Audits and Recordkeeping

Section 202.1002 authorizes DOJ to require audits of compliance with the rule's requirements, and Subpart K imposes recordkeeping and reporting for restricted

[10] Id. at 108.

transactions. Entities must maintain documentation demonstrating their data flows and due diligence (similar to OFAC sanctions compliance records).[11] DOJ expects companies to build policies and controls (e.g., internal audits, verification procedures) to ensure "the final rule's due diligence provisions" are met.[12] Operationalizing compliance should resemble building a specialized export-control compliance regime for data, requiring coordination between legal, IT, and operational teams.

Advisory Opinions and Exemptions

The rule includes an advisory opinion process, at 28 CFR 202.900 et seq., for uncertain cases, providing a safety valve for industry. It also carves out certain exemptions (e.g., federal government business, non-sensitive data, transactions initiated by U.S. government agencies). Importantly, DOJ leaves the flexibility of "reasonable" due diligence up to each business; entities must tailor their processes to their risk profile.[13] Companies should assess whether it should seek advisory opinions and carefully consider the exemptions.

CONTRACTUAL AND COMMERCIAL CONSIDERATIONS

Vendor and Processor Contracts

Businesses will need to update contracts to address the rule. Likely measures include:

(1) Clauses prohibiting transfers of covered data to countries of concern;

(2) Requiring immediate notification of any (potential) covered transaction;

(3) Granting the right to audit compliance with the rule; and

(4) Limitations and restrictions on the use of anonymized, aggregated, or de-identified data.

Companies should consider adding clauses that mirror the rule's sanctions clauses and forbidding any prohibited "transactions" with designated countries/parties. Also, due diligence obligations must flow down the chain: e.g., a data broker contracting with a processor should require that processor to screen for covered data flows and pass down the same contractual restrictions.

---

[11] 31 C.F.R. pts. 501 & 515 (2025).

[12] See 90 Fed. Reg. 1,636, 28 (Jan. 8, 2025), supra note 6.

[13] Id. at 108

Model Contractual Clauses for Compliance

Any U.S. persons engaging in data transactions involving data brokerage with foreign persons (who are not covered persons) must include contractual language prohibiting the foreign person from engaging in the onward transfer or resale of government-related data or bulk U.S. sensitive personal data to countries of concern or covered persons.

The DOJ Compliance Guide provides the following language as an example of a model contractual clause:

> [U.S. person] provides [foreign person] with a non-transferable, revocable license to access the [data subject to the brokerage contract]. [Foreign person] is prohibited from engaging or attempting to engage in, or permitting others to engage or attempt to engage in the following:
>
> (a) selling, licensing of access to, or other similar commercial transactions, [such as reselling, sub-licensing, leasing, or transferring in return for valuable consideration,] the [data subject to the brokerage contract] or any part thereof, to countries of concern or covered persons, as defined in 28 CFR part 202;
>
> Where [foreign person] knows or suspects that a country of concern or covered person has gained access to [data subject to the brokerage contract] through a data brokerage transaction, [foreign person] will immediately inform [U.S. person]. Failure to comply with the above will constitute a breach of [data brokerage contract] and may constitute a violation of 28 CFR part 202.[14]

While the DOJ provides the above language as an example of contractual language that may be considered when U.S. persons are engaging in data transactions, the DOJ acknowledges that parties may wish to tailor their contractual language based on several factors, including the relevant business activity, risk appetite, the contract counterparties, the products and services involved, and the bulk U.S. personal sensitive or government-related data at issue. Companies should assess which data transaction needs to be renegotiated to include the DOJ-required provisions and whether master service agreements and agreement templates should be revised to include such terms for transactions moving forward.

Potential contractual considerations include:

- Representations and warranties that the vendor will not transfer, allow access to, or process "bulk U.S. sensitive personal data" on behalf of or for the benefit of a "country of concern."

[14] U.S. Dep't of Justice, Nat'l Sec. Div., Data Security Program: Compliance Guide 1 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396356/dl (last visited June 16, 2025).

- Covenants to conduct appropriate geographic and end-use due diligence on subcontractors or recipients.
- Notification and audit provisions allowing the primary data controller to verify compliance with EO 14117 obligations.
- Clauses explicitly recognizing that anonymized, de-identified, or pseudonymized data is still in-scope for regulatory purposes under the DOJ rule and/or restricting vendor ability to create derivative data of this kind.
- Indemnification clauses (1) covering regulatory enforcement or litigation arising from unauthorized data transfers or improper anonymization practices and (2) for breach of the reps and warranties.
- Termination rights in the event of violations or inability to maintain adequate safeguards.
- Adequate insurance coverage for cyber errors and omissions.

Data Brokerage Agreements

While the DOJ requires U.S. persons to reevaluate and renegotiate data transaction agreements with foreign persons, the rule explicitly prohibits U.S. persons from engaging in data transactions involving data brokerage with covered persons or countries of concern. The DOJ Compliance Guide states that: "Inclusion of contractual language regarding use or onward sale of the data will not authorize a U.S. person to engage in such a transaction with a covered person or country of concern."[15]

Data brokers (§202.301), broadly defined, are prohibited from selling or transferring Americans' personal data in bulk to covered persons. Thus, agreements for data sales or access may need re-structuring. For example, a broker's contracts with foreign buyers will need explicit compliance language (and perhaps pricing adjustments to account for limits). Similarly, U.S. companies buying large data sets should ensure sellers have vetted the origin and legal status of the data.

Supply Chain Procedures

The DOJ rules also require additional supply chain procedures. Due diligence in transactions (mergers, investments, vendor onboarding) should include screening for "countries of concern" issues for data transactions, akin to Committee on Foreign

[15] See footnote 14. U.S. Dep't of Justice, Nat'l Sec. Div., Data Security Program: Compliance Guide 1 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396356/dl (last visited June 16, 2025).

Investment in the United States (CFIUS)[16] or foreign investment analysis.[17] Entities may require contractual representations about not being owned/controlled by relevant adversaries. Any capital or joint-venture agreements may involve commitments not to cause covered data transfers.

ANONYMIZED, DE-IDENTIFIED, AND PSEUDONYMIZED DATA UNDER DOJ RULE VS. GLOBAL PRIVACY LAWS

DOJ's Broad Treatment

Unlike most U.S. privacy laws, the DOJ rule does *not* exclude anonymized, pseudonymized, or de-identified data. In comments, DOJ refused to carve out these categories, stating that "even anonymized data, when aggregated, can be used by countries of concern… to identify individuals and conduct malicious activities,"[18] and the subsequently published FAQ reiterates this point.[19] In fact, the final rule explicitly treats any attempt at anonymization or pseudonymization as still "sensitive personal data" if the bulk criteria are met.[20] Thus, covered entities cannot rely on data-sanitization to escape the rule.

CCPA and State Laws

In contrast, U.S. consumer privacy statutes generally exempt de-identified data. For example, the California Consumer Privacy Act, as amended from time to time, including but not limited by the California Privacy Rights Act and the applicable regulations (collectively, CCPA) defines "deidentified" information as that which "cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer," subject to a public commitment not to re-identify. CCPA likewise defines "pseudonymization" as processing that renders data "no longer attributable" to a person without separate data. Under these laws, data that meets the technical standards of de-identification is outside the law's scope. By contrast, DOJ's rule sidesteps those distinctions and keeps deidentified data in play whenever it is sufficiently voluminous.

---

[16] 31 C.F.R. §§ 800.209, 800.241 (2025) (defining covered transactions and outlining categories of sensitive personal data under CFIUS regulations).

[17] Exec. Order No. 14,105, 88 Fed. Reg. 54,867 (Aug. 11, 2023) (addressing U.S. outbound investment screening in sensitive technologies); U.S. Dep't of the Treasury, Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern (ANPRM), 88 Fed. Reg. 54,961 (Aug. 14, 2023) (foreign investment due diligence now includes evaluating data-related risks).

[18] See Final Rule, supra note 6, at 108.

[19] U.S. Dep't of Justice, Nat'l Sec. Div., Data Security Program: FAQs #22 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396351/dl (last visited June 16, 2025).

[20] See Final Rule, supra note 6, at 105.

Practical impact of this consideration is that data strategies valid under CCPA/ (e.g., using pseudonymization for secondary purposes or as research data) may need to be revisited. Even HIPAA-compliant de-identified health data, if aggregated beyond the DOJ's thresholds, may count as "sensitive personal data" under this regime. This heightens compliance burdens, especially for sectors (health, genomics, finance, location services) that routinely work with large, ostensibly anonymized datasets.

GDPR Anonymization vs. Pseudonymization

To continue the analysis with other global privacy laws, the EU General Data Protection Regulation (GDPR) draws a firm line: truly anonymized data (irreversibly stripped of identifiers) falls outside the regulation, whereas pseudonymized data remains personal data because re-identification is possible. The definition of "anonymous data" under GDPR is itself contested, and some acknowledge that residual risks remain even in purportedly anonymized datasets.[21] By contrast, pseudonymization (Art. 4(5) GDPR) is a recognized security technique (Art. 89) and does not exempt data from GDPR – it merely permits certain processing under stricter safeguards.

Under GDPR, a company may treat data as non-personal-data if re-identification risk is effectively eliminated. In contrast, the DOJ rule assumes that no anonymization is risk-free due to the national security concerns at play: any large dataset of sensitive personal data is treated as in-scope.

CISA Requirements and Data Minimization Techniques

Because most U.S. state consumer privacy laws as well as the GDPR and most other global privacy laws exempt de-identified data, complying with the DOJ rule would require a new data compliance program with different sets of requirements in terms of the data transactions that may be in scope. This divergence means multinational companies must navigate dual regimes: they may be permitted by privacy regulators to use pseudonymized data, yet restricted from sharing it under the national-security rule. In practice, U.S. companies doing business internationally will need to meet both sets of requirements if they want to leverage de-identified data.

While this article focuses on the rule's impact on data transactions and contracting requirements, companies should carefully consider the Cybersecurity and Infrastructure Security Agency (CISA) Security Requirements for Restricted Transactions, which the U.S. CISA published to set out the security requirements companies must implement for restricted transactions.[22]

[21] Michèle Finck & Frank Pallas, They Who Must Not Be Identified – Distinguishing Personal from Non Personal Data under the GDPR, 10 Int'l Data Privacy L. 11 (2020), https://doi.org/10.1093/idpl/ipz026.

[22] Cybersecurity & Infrastructure Sec. Agency, Security Requirements for Restricted Transactions 1 (Jan. 3, 2025), https://www.cisa.gov/sites/default/files/2025-01/Security_Requirements_for_Restricted_Transaction-EO_14117_Implementation508.pdf (last visited June 16, 2025).

Specifically, while the DOJ Compliance Guide and FAQ are clear that anonymization and pseudonymization would not bring the data out of scope of the rule, the CISA requirements state that implementing a combination of data minimization and data masking strategies could be considered by companies to prevent visibility into that data and thus prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable. According to the CISA guidance, this may be achieved through application of techniques such as aggregation, pseudonymization, de-identification, or anonymization.[23]

Since companies have significant interest in identifying which transactions are prohibited, restricted, or allowable, careful consideration of the DOJ Final Rule together with the CISA Security Requirements will help to understand how companies can continue to operate with data transactions that are restricted by following the CISA guidance.

EXECUTIVE ORDERS AS FEDERAL DATA PRIVACY POLICY TOOLS

EOs in Privacy Policy

EO 14117 exemplifies the growing reliance on executive action for privacy/national-security regulation in absence of omnibus privacy legislation at the federal level. The executive branch has used increasingly "nationalized" personal data governance (e.g., Team Telecom,[24] TikTok-related measures[25]) using IEEPA and other authorities.[26] EO 14117, like the Protecting Americans' Data from Foreign Adversaries Act (PADFA) signed concurrently, to create a statutory/regulatory patchwork aimed at the same goals.

ENFORCEMENT AUTHORITY AND PENALTIES

IEEPA Enforcement

DOJ will enforce the rule under IEEPA (50 U.S.C. § 1705) and associated regulations. Violations can incur civil fines (up to $250,000 per violation) and criminal penalties up to 20 years of imprisonment.[27]

---

[23] Id.

[24] U.S. Dep't of Justice, Nat'l Sec. Div., Team Telecom (last updated Sept. 20, 2023), https://www.justice.gov/nsd/team-telecom (last visited June 16, 2025).

[25] Extending the TikTok Enforcement Delay, Exec. Order No. 14,258, 90 Fed. Reg. ___, ___ (Apr. 4, 2025), https://www.whitehouse.gov/presidential-actions/2025/04/extending-the-tiktok-enforcement-delay/ (last visited June 16, 2025).

[26] Anupam Chander & Paul M. Schwartz, The President's Authority Over Cross Border Data Flows, 172 U. Pa. L. Rev. 1989 (2024), https://doi.org/10.2139/ssrn.4937884.

[27] 50 U.S.C. § 1705 (2022).

Analogous Regimes

While novel in the privacy context, this regime resembles other national-security rules (e.g., CFIUS powers over "critical technology" transfers, and existing export controls on encryption or data surveillance tech). Importantly, unlike FTC or state attorneys general enforcement of privacy laws, this rule implicates criminal authorities and is backed by broad IEEPA powers.

CONCLUSION

The DOJ's Rule implementing Executive Order 14117 signals a major shift in U.S. data governance, extending national security scrutiny beyond traditional foreign investment and export control frameworks into the realm of private sector data practices. By treating anonymized, pseudonymized, and de-identified data as subject to regulatory thresholds, the Rule expands upon existing U.S. consumer privacy paradigms. Legal practitioners and organizations must now incorporate national security-focused due diligence, transactional controls, and contractual risk allocation into their data governance frameworks – particularly when handling sensitive data categories at scale. In the context of AI development, cross-border data services, and third-party vendor engagement, this Rule raises the stakes for data compliance, requiring legal teams to develop a granular understanding of the intersection between privacy, security, and geopolitical risk.