

AN A.S. PRATT PUBLICATION

JULY-AUGUST 2025

VOL. 11 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT



LexisNexis

**EDITOR'S NOTE: LET'S LOOK AT WHAT'S
HAPPENING IN THE STATES**

Victoria Prussen Spears

**MORE STATES PROPOSE PRIVACY LAWS
SAFEGUARDING NEURAL DATA**

Linda K. Clark and Carson Martinez

**CALIFORNIA COURT REJECTS ATTEMPT TO
EXPAND THIRD-PARTY EAVESDROPPING
CLAIMS TO INTERNET COMMUNICATIONS:
HOW YOUR BUSINESS CAN MITIGATE RISK**

Catherine M. Contino and Usama Kahf

**COURT CONFIRMS KENTUCKY CONSUMER
PROTECTION ACT DOES NOT COVER
EMPLOYEES, BUT LEGAL RISKS REMAIN:
5 STEPS FOR EMPLOYERS TO AVOID
DATA BREACH LAWSUITS**

Annie N. Harb

**U.S. DEPARTMENT OF JUSTICE IMPLEMENTS
BULK PERSONAL DATA TRANSFER RESTRICTIONS**

Artie McConnell, Eric B. Gyasi, Gerald J. Ferguson
and Jennifer G. Solari

**UK'S ECONOMIC CRIME AND CORPORATE
TRANSPARENCY ACT 2023 INTRODUCES
IDENTITY VERIFICATION REGIME**

Harry Keegan, Vance Chapman,
George O'Malley, Kelvin Mahal and
Amy Hughes

**EUROPEAN HEALTH DATA SPACE
REGULATION PUBLISHED IN THE
EU OFFICIAL JOURNAL**

Alexander Roussanov and
Ana Gonzalez-Lamuño

**CHINA DATA PRIVACY: NEW CLARITY ON
AUDIT AND DATA PROTECTION OFFICER
REQUIREMENTS**

Paul D. McKenzie, Gordon A. Milner,
Chuan Sun and Tingting Gao

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11

NUMBER 6

July-August 2025

Editor's Note: Let's Look at What's Happening in the States Victoria Prussen Spears	165
More States Propose Privacy Laws Safeguarding Neural Data Linda K. Clark and Carson Martinez	167
California Court Rejects Attempt to Expand Third-Party Eavesdropping Claims to Internet Communications: How Your Business Can Mitigate Risk Catherine M. Contino and Usama Kahf	172
Court Confirms Kentucky Consumer Protection Act Does Not Cover Employees, But Legal Risks Remain: 5 Steps for Employers to Avoid Data Breach Lawsuits Annie N. Harb	176
U.S. Department of Justice Implements Bulk Personal Data Transfer Restrictions Artie McConnell, Eric B. Gyasi, Gerald J. Ferguson and Jennifer G. Solari	180
UK's Economic Crime and Corporate Transparency Act 2023 Introduces Identity Verification Regime Harry Keegan, Vance Chapman, George O'Malley, Kelvin Mahal and Amy Hughes	186
European Health Data Space Regulation Published in the EU Official Journal Alexander Roussanov and Ana Gonzalez-Lamuño	192
China Data Privacy: New Clarity on Audit and Data Protection Officer Requirements Paul D. McKenzie, Gordon A. Milner, Chuan Sun and Tingting Gao	199

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@lexisnexus.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.lexisnexus.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)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2025 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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.lexisnexus.com

MATTHEW  BENDER

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES

Partner, Venable LLP

CHRISTOPHER G. CWALINA

Partner, Holland & Knight LLP

RICHARD D. HARRIS

Partner, Day Pitney LLP

JAY D. KENISBERG

Senior Counsel, Rivkin Radler LLP

DAVID C. LASHWAY

Partner, Sidley Austin LLP

CRAIG A. NEWMAN

Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL

Partner, Sidley Austin LLP

RANDI SINGER

Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI

Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE

Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH

Partner, Thompson Hine

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. Copyright 2025 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries 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.

U.S. Department of Justice Implements Bulk Personal Data Transfer Restrictions

*By Artie McConnell, Eric B. Gyasi, Gerald J. Ferguson and Jennifer G. Solari**

In this article, the authors highlight key features of the Data Security Program implemented by the U.S. Department of Justice's National Security Division and recommend steps that companies can take to prepare for enforcement.

The Data Security Program (DSP) recently implemented by the U.S. Department of Justice (DOJ) will have far-reaching implications for many businesses that transfer the personal data of U.S. citizens outside the United States. This article highlights key features of the DSP and recommends steps that companies can take to prepare for enforcement.

THE DATA SECURITY PROGRAM'S KEY PROVISIONS

Types of Covered Data

The DSP creates two categories of covered data: bulk sensitive personal data of U.S. persons and government-related data. The rule establishes six categories of "sensitive personal data":

1. Covered personal identifiers (e.g., demographic information, contact information, and device identifiers when combined with other covered personal identifiers);
2. Precise geolocation data (more expansive than most state privacy law definitions);
3. Biometric identifiers;
4. Human 'omic data;
5. Personal health data; and
6. Personal financial data.

The DSP does not exempt pseudonymized, anonymized or de-identified data from the definition of personal sensitive data.

* The authors, attorneys with Baker & Hostetler LLP, may be contacted at amcconnell@bakerlaw.com, egyasi@bakerlaw.com, gferguson@bakerlaw.com and jsolari@bakerlaw.com, respectively.

For each of the above categories, thresholds are established to quantify “bulk,” as illustrated in Table 1. To make the determination of whether a transaction meets the bulk threshold, all transactions for the preceding 12 months are aggregated.

Table 1

<i>Sensitive Data Category</i>	<i>Bulk Threshold</i>
Human Genomic Data	Over 100 U.S. persons
Human ‘omic Data	Over 1,000 U.S. persons
Biometric Identifiers	Over 1,000 U.S. persons
Precise Geolocation	Over 1,000 U.S. devices
Personal Health Data	Over 10,000 U.S. persons
Personal Financial Data	Over 10,000 U.S. persons
Certain Covered Personal Identifiers	Over 10,000 U.S. persons

Covered Data Transactions

The DSP defines covered data transactions as those transactions involving bulk U.S. sensitive personal data or government-related data.

- Each type of transaction is categorized as either prohibited or restricted.
 - The DSP provides specific definitions for data brokerage, vendor agreements, employment agreements and investment agreements.
 - The DSP prohibits data brokerage transactions but provides allowances for vendor agreements, employment agreements, and investment agreements – as long as the transfers are subject to certain security requirements.
- Exemptions – The DSP provides for certain types of transactions which are otherwise covered data transactions but are exempt transactions (e.g., personal communications, financial services, telecommunication services, and corporate group transactions).

COUNTRIES OF CONCERN AND COVERED PERSONS

- *Countries of Concern:* The DSP identifies the countries of concern as China, Russia, Iran, North Korea, Cuba and Venezuela.
- *Covered Persons:* Those entities which are 50 percent or more owned, directly or indirectly or in the aggregate, by one or more countries of concern or covered persons or that are organized or chartered under the laws of, or have their principal place of business in, a country of concern.

“KNOW-YOUR-DATA” AND DILIGENCE REQUIREMENTS

- *Know-Your-Data Requirement*: This provision goes into effect October 6, 2025. By that time, companies that participate in restricted transactions must design and implement a compliance program which contains the following elements:
 - Risk-based procedures to verify data flows that are auditable and identify:
 - (i) The types and volume of covered data involved in that transaction;
 - (ii) The transaction parties; and
 - (iii) The ultimate use of the data and how the data was transferred.
 - A risk-based process for identifying vendors.
 - Written data compliance program policies that are certified annually by an officer, executive, or other employee who has responsibility for compliance.

THE DSP'S GUIDANCE

On April 11, 2025, DOJ announced the next steps in the implementation of DSP.¹ NSD also issued a Compliance Guide,² an initial list of over 100 Frequently Asked Questions,³ and an Implementation and Enforcement Policy for the first 90 days.⁴ An initial Covered Persons List that identifies and designates people and entities “subject to the control and direction of foreign adversaries” is forthcoming.

It is important to note that the DSP is a national security directive, not a privacy regulation designed to protect individual privacy or interests. Not surprisingly, in issuing the April 11, 2025 guidance, DOJ noted that the DSP “establishes what are effectively export controls” governing the sensitive data and foreign parties at issue.

Indeed, compliance practitioners and litigators who handle sanctions and export control matters will find much about the DSP that is familiar: the DSP closely tracks the restrictions, oversight, licensing and enforcement frameworks used by the Department of the Treasury’s Office of Foreign Assets Control (OFAC) and the Department of Commerce’s Bureau of Industry and Security (BIS) governing the flow of goods and funds to and involving foreign entities.

¹ <https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive>.

² <https://www.justice.gov/opa/media/1396356/dl>.

³ <https://www.justice.gov/opa/media/1396351/dl>.

⁴ <https://www.justice.gov/opa/media/1396346/dl?inline>.

NEXT STEPS FOR YOUR COMPANY

Given this context and precedent, there are steps that U.S. businesses should consider taking to ensure compliance with the DSP and minimize potential disruptions to their business.

- *Know Your Data:* Identify and classify categories of data that fall under the rule and assess whether it is stored, processed or transmitted in ways that could be accessed by covered persons. Per the April 11, 2025 guidance, the covered persons analysis mirrors the “50% Rule” OFAC uses to identify sanctioned parties. The guidance also describes how combinations of data can trigger the rule, including things like IP addresses, mobile device IDs, MAC addresses and mobile advertising IDs together with other identifiers.
- *Restrict Access:* Review relationships with vendors and identify potential access by foreign subsidiaries and third parties, such as IT service contractors, data analytics providers and offshore cloud storage. Where appropriate, implement access controls and logging mechanisms.
- *Gap and Security Assessments:* To ensure compliance with the CISA security requirements (which were updated in conjunction with the DSP), conduct a gap assessment to identify noncompliant processes and procedures (including the requirement for asset inventories, updated software and hardware, and remediation timelines for vulnerability patching).
- *Prepare for Audits and Reporting:* Document your organization’s data flow and ensure appropriate policies and procedures to identify potentially covered transactions. At a minimum, when conducting due diligence on data transfers to prevent unauthorized downstream access, make sure that such efforts are preserved and can be retrieved in the future.
- *Update and Revise Contract Language:* Contractual protections can be effective tools to manage and allocate compliance risk when sharing data with third parties, vendors or foreign affiliates. The April 11, 2025 Compliance Guide provides model contractual language that should be implemented immediately and, where possible, incorporated into existing relationships. Should a relationship or contract require termination to comply with the DSP, companies must be mindful of litigation risks, as compliance with EO 14117 and the DSP will not necessarily constitute a force majeure event.
- *Contact NSD with Questions and Requests for Clarification:* During this 90-day period, NSD encourages the public to contact them with informal inquiries about the DSP. While NSD will not be able to respond to every inquiry, the mere fact that a company sought clarification about the DSP or guidance regarding a third-party relationship or transaction, evinces

good faith and reasonableness that, in the event of an inadvertent breach, can be cited as evidence of attempted compliance.

- *Prepare Specific License Requests:* The DSP tracks OFAC's approach to "general" and "specific" licenses. Companies should prepare any specific license applications as far in advance as possible, as similar requests with BIS and OFAC typically take months to be processed and frequently require extensive communications between the government and the applicant.

IN SUMMARY

- Under Executive Order 14117, the U.S. Department of Justice's (DOJ) National Security Division (NSD) has implemented a Data Security Program (DSP) to address national security risks associated with foreign access to sensitive U.S. data.⁵
- The DSP is designed to "prevent China, Russia, Iran, and other foreign adversaries from using commercial activities to access and exploit . . . Americans' sensitive personal data to commit espionage, conduct surveillance and counterintelligence activities . . . and otherwise undermine our national security."
- The DSP is a national security directive, not a privacy regulation designed to protect individual privacy or interests. As a result, the DSP contains many characteristics that are similar to U.S. sanctions and export control regimes.
- The DSP's regulations became effective on April 8, 2025, with certain compliance requirements taking effect 90 days later on July 7, 2025.
- Companies that collect this sort of data are now subject to restrictions traditionally reserved for the defense sector and other highly sensitive government contracts. Failure to comply can result in DOJ inquiries and enforcement, including civil and criminal liability under the International Emergency Economic Powers Act (IEEPA) and other statutes. Civil violations can lead to fines of up to \$366,136 (or an amount equal to twice the amount of the sanctioned transaction), while criminal penalties can include imprisonment for up to 20 years and a \$1,000,000 fine.

⁵ <https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related>. The DOJ issued a Final Rule implementing EO 14117 on January 8, 2025. See <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>

CONCLUSION

As with other national security-focused initiatives, the DSP creates a variety of compliance challenges that transcend traditional practice areas and implicate a variety of cybersecurity, international trade and white collar litigation issues. As U.S. businesses adjust, the touchstones for compliance are, and will remain, good faith, reasonable and proportionate steps, and due diligence. Such an approach, consistent with the April 11, 2025 guidance, will not only minimize the risk of noncompliance with the DSP but also help protect a company and its partners in the event of a government inquiry down the road.