Act before the notice arrives — Managing regulatory and litigation risk under the Bulk Data Transfer Rule

By Hope Anderson, Esq., David Lim, Esq., and Burak Haylamaz, Esq., White & Case LLP

AUGUST 7, 2026

The Department of Justice ("DOJ")'s Bulk Sensitive Data Transfer Rule (the "Rule") is no longer forthcoming, it is here. Originating from Executive Order 14117 and codified at 28 C.F.R. Part 202, all elements of the Rule have been fully effective since October 6, 2025. It restricts, and in some cases outright prohibits, transactions involving bulk sensitive personal data or U.S. government-related data between U.S. persons and designated countries of concern or their affiliated entities and individuals.

The Rule's reach extends across industries, touching routine business arrangements in employment, vendor management, and investment. For companies that have treated the Rule as a future compliance problem, that future has arrived. Enforcement is active, penalties are significant, and the litigation landscape is expanding well beyond the DOJ's own enforcement mechanisms.

What the Rule covers: A practical refresher

The threshold question for any company is whether its existing data flows fall within the Rule's scope. At its core, the Rule is designed to reduce national security risks by restricting and, in some cases, outright prohibiting certain transactions involving U.S. sensitive personal data or U.S. government-related data ("covered data") with countries of concern or their affiliated covered persons.

The six countries of concern currently designated under the Rule are China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela. The Rule also restricts access by "covered persons" that captures: (i) individuals who reside in or are employed by entities in countries of concern; (ii) entities that are organized or chartered under the laws of, or have their principal place of business in, a country of concern, or are owned 50% or more by such entities.

On the data side, the Rule draws a distinction between two categories of covered data. U.S. government-related data, which includes precise geolocation data for areas designated as posing a heightened national security risk and personal data linked to current or former U.S. government employees, is subject to the Rule regardless of volume.

U.S. sensitive personal data, by contrast, only triggers the Rule once it crosses defined "bulk" thresholds measured over the preceding 12-month period, aggregated across all transactions with the same counterparty. The six covered data categories and their respective thresholds range from human 'omic data (as low as 100 U.S. persons for genomic data) to biometric identifiers, precise geolocation data, personal health data, personal financial data, and covered personal identifiers.

The Bulk Sensitive Data Transfer Rule restricts, and in some cases outright prohibits, transactions involving bulk sensitive personal data or U.S. government-related data between U.S. persons and designated countries of concern or their affiliated entities and individuals.

These are not edge-case data types. They are routinely collected through mobile applications, HR platforms, employee benefits systems, and commercial data arrangements, making the Rule relevant to a broad cross-section of industries. The Rule applies whether the data is de-identified or not, a distinction from many US state privacy laws.

The compliance framework: Obligations that are now enforceable

The Rule creates two tiers of covered transactions: prohibited transactions and restricted transactions. Unless exempt or authorized otherwise, the Rule prohibits any covered data brokerage involving covered data with covered persons, and any transaction involving access to bulk human 'omic data or biospecimens from covered persons.

Restricted transactions, which arise from employment agreements, vendor agreements, or investment agreements that give covered persons access to covered data, are permissible only if the U.S. person engaging in them satisfies

a set of affirmative compliance requirements. Those requirements are now fully in force.

U.S. persons conducting restricted transactions must: (i) comply with the Cybersecurity and Infrastructure Security Agency ("CISA") security requirements (https://bit.ly/45r54ED), which impose organizational, system, and data-level safeguards specifically designed to prevent covered persons from accessing covered data ; (ii) develop, implement, and routinely update a risk-based, written Data Compliance Program designed to prevent, detect, and remediate violations; (iii) conduct an annual independent audit that evaluates the effectiveness of the Data Compliance Program and identifies any security vulnerabilities; and (iv) maintain complete records of each restricted transaction for at least 10 years.

Enforcement is active, penalties are significant, and the litigation landscape is expanding well beyond the DOJ's own enforcement mechanisms.

Notably, these requirements are not regulatory expectations, or industry best practices. They are binding conditions on the lawfulness of restricted transactions, and a failure to implement them is itself a violation of the Rule.

Enforcement is real and the litigation risk extends beyond the DOJ

The consequences of non-compliance are significant and, in serious cases, severe. Civil penalties for violations are substantial, with the amount not exceeding the greater of $377,700 (adjusted for inflation) or twice the value of the transaction that forms the basis of the violation. In cases of willful violations, criminal penalties can be severe, including a fine of up to $1 million, imprisonment for up to 20 years, or both.

Equally important is the emerging civil litigation risk. Although the Rule does not contain a private right of action, plaintiffs' counsel have moved quickly to identify other avenues of recourse. Over the past year, multiple plaintiffs have filed lawsuits alleging that companies violated the Electronic Communications Privacy Act ("ECPA") by intercepting users' communications and transmitting sensitive personal data to entities linked to countries of concern, including *Baker v. Index Exchange* (U.S. District Court for the Northern District of Illinois, filed 2025) (The court denied Index Exchange's motion to dismiss on June 16, 2026, allowing the case to proceed into discovery and further pretrial proceedings.) *Porcuna v. Xandr* (U.S. District Court for the Northern District of California, filed 2025) (Xandr's motion to dismiss the First Amended Complaint remains pending, with briefing completed and a hearing scheduled.) and *McGrath v. Google LLC*, (U.S. District Court for the Northern District of California, filed 2026) (The case has been consolidated into the broader *In re Google Bulk Sensitive Data Rule Litigation* proceedings.)

As a recall, under ECPA, an interception is not unlawful if at least one party gave prior consent, unless the communication was intercepted for the purpose of committing a criminal or tortious act, in which case the interception is unlawful notwithstanding any prior consent (the "crime-tort exception"). Plaintiffs characterize those transfers as violations of the Rule and seek to invoke ECPA's crime-tort exception by using the regulatory violation as the predicate crime or tort, thereby converting a compliance failure into an independent civil cause of action.

While these cases remain in their early stages, their volume and the consistency of the underlying theory signal that plaintiffs' firms view the Rule as a durable source of litigation leverage. Companies without documented compliance programs, adequate internal controls, and evidence of good-faith remediation will therefore have limited grounds on which to defend against these claims.

The stakes of inaction

Some companies may be inclined to wait to see which industries the DOJ targets first, or how the courts resolve the emerging ECPA litigation. That instinct is understandable, but it is strategically unsound. By the time a company receives a pre-penalty notice from the DOJ, or is named in an ECPA complaint, its compliance posture will already be on the record.

The DOJ has made its expectations clear, noting "U.S. persons should "know their data" and the front-line role they play in mitigating these risks," in a press release. Given this clear benchmark, a compliance program hastily assembled in response to an enforcement inquiry is not a defense; it is an admission that one did not exist when it should have.

Therefore, the appropriate starting point is a deliberate assessment of whether the Rule applies, including detailed data mapping: what data does the company collect and at what volumes, what counterparties have access to it, and do any existing employment, vendor, or investment agreements create restricted transactions?

From there, companies should build or update their Data Compliance Programs, including drafting a Compliance Policy, implementing the applicable CISA security requirements, amending vendor contracts to include the required downstream transfer restrictions, and establishing the annual audit and certification cycle required by the Rule.

The Rule is in effect. The enforcement posture is live. The litigation risk is real and growing. Companies that act now, deliberately and with appropriate legal guidance, will therefore be materially better positioned to withstand regulatory scrutiny and manage litigation exposure than those that continue to wait.

About the authors



Hope Anderson (L) is the office executive partner for the Los Angeles office of **White & Case LLP** and serves as co-head of the firm's artificial intelligence practice. She can be reached at hope.anderson@whitecase.com. **David Lim** (C) is a partner in the firm's global international trade practice and a former US Department of Justice official who held multiple senior roles related to sanctions and export controls. At the firm, he advises clients on complex cross-border national security matters. He is based in Washington, D.C. **Burak Haylamaz** (R) is a staff attorney based in the Los Angeles office of the firm and is a member of the firm's tech disputes and data, privacy and security practice groups. He can be reached at burak.haylamaz@whitecase.com.

This article was first published on Reuters Legal News and Westlaw Today on August 7, 2026.