Bloomberg Law News 2026-03-12T10:35:0390658369-04:00

China-Focused Bulk Data Rule Sparks New Risk for Pixel Tracking

By Ufonobong Umanah 2026-03-12T05:00:10000-04:00

A recently implemented national security regulation restricting the transfer of sensitive US personal data to hostile foreign regimes—particularly China—presents new legal challenges for companies engaged in online advertising.

The Bulk Sensitive Data Rule, finalized in April of last year, prohibits or restricts the transmission of bulk data to China and five other countries in a variety of contexts. It stems from a Biden-era executive order directing the Justice Department to issue regulations to restrict access to US data where it would pose an unacceptable national security risk.

US lawmakers on both sides of the aisle have repeatedly expressed concerns about China-based companies collecting American data. Those concerns helped drive the US to force Bytedance to sell TikTok's American operations, while attorneys general across US states have sued Chinese firms under various consumer protection and privacy laws.

But the BDSR has ushered in a new challenge: lawsuits from private parties.

The first two privatelawsuits for alleged illegal transfers under the rule—against a Microsoft Corp. subsidiary and digital advertiser Index Exchange Inc.—were filed in September, followed by seven more complaints in February and an eighth in March, including against Google LLC, Lenovo Group Ltd., and four other companies.

The regulation's complexity may have meant plaintiffs' firms needed time to understand how to leverage the rule for use in private suits, which would explain the sudden recent wave, said Elizabeth J. McEvoy of Epstein Becker & Green PC.

"If you're engaged in sharing data cross- border that's personal to US citizens and you're sharing it directly with one of those six countries of concern, or someone residing in those countries, you should stop and do an analysis of whether you're running afoul of the sensitive data rule," said McEvoy, who

represents large academic medical centers and private companies.

The lawsuits are only one pressure point, as nine of them came ahead of a March 1 deadline for some companies to file annual reports describing some of their data transactions.

“We will see an increase in 2026 in government enforcement” as the US evaluates those reports, McEvoy said.

A broad range of companies, even if they aren’t directly tied to national security, could be caught up by the BDSR, and some are starting to take notice, said Sam Castic of Hintze Law LLC. The private suits raise the risk profile for any company using trackers for advertising who send data collected by those programs—or are perceived to—to China, he said.

Same Claims, New Hook

Data collected for advertising is a prominent concern in the BSDR, which classifies the use of tracking pixels or software development kits as “data brokerage.”

So is providing a certain number of IP addresses and advertising IDs to marketers or advertising exchanges based in China. Subject to certain exemptions—such as for travel and financial services—data brokerage with the listed countries of concern is prohibited.

All 10 private lawsuits say the defendants violated the Electronic Communications Privacy Act by deploying a host of online trackers on their webpages to intercept visitor communications and transmit them to third parties, including in some cases China-based Temu and ByteDance.

There isn’t a private right of action under the BSDR—meaning only the government can enforce it—so plaintiffs are using ECPA to get in the courthouse door, Castic said.

ECPA allows individuals to sue for impermissibly intercepting their communications, but ordinarily shields parties to a communication from liability.

Litigants argue that the crime-tort exception—which removes the liability shield if the data is collected for the purpose of committing a crime or tort—applies, making collecting companies liable for

transmitting data to the countries targeted by the BSDR.

Plaintiffs have used substantive privacy laws to target data transfers that allegedly violate the Health Insurance Portability and Accountability Act, which also lacks a private right of action, in the same way, McEvoy said. Suits that do so often allege that trackers installed on health-care websites collect personal health information, which HIPAA generally prohibits disclosing to others.

Leverage Point

Such suits might prove difficult for companies to shake off quickly, she said. The BSDR provides plenty of guidance as to what data is permissible to share and what isn't, and leaves less room for flexible interpretation.

"I don't think that the narrative that the practices would violate the DOJ rule necessarily gets the plaintiffs very far in terms of proving the underlying claims," Castic said.

Instead, the cases will likely rise or fall based on whether plaintiffs can sufficiently allege the elements of the cited laws, he said.

But "I do think that many companies have started to apply more scrutiny and due diligence to the types of partners they're working with that they allow to have those tracking technologies in their app or on their site," he said.

And there has been a move to steer clear of companies based in countries of concern in light of the BSDR, he said.

Plaintiffs may take the BSDR, intended as a national security tool, and "stretch its original intent" as part of a broader litigation strategy as the lawsuits ramp up, said R Street Institute Resident Fellow of Cybersecurity and Emerging Threats Haiman Wong said.

How judges rule in these early cases "could have significant implications not only for how companies interpret their compliance obligations, but also for how national security-driven data governance rules evolve going forward," she said.

To contact the reporter on this story: Ufonobong Umanah in Washington at uumanah@bloombergindustry.com

To contact the editors responsible for this story: Nicholas Datlowe at ndatlowe@bloombergindustry.com; Laura D. Francis at lfrancis@bloombergindustry.com

Related Articles

TikTok's Fate Rests on Trump After Supreme Court Upholds Law (2)

Web Ad Firms Sued Under Biden Rule Over China Data Transfers (1)

TikTok Seals Deal to Operate in the US After Years of Drama (2)

Lenovo Hit With Suit for Breaking US Bulk Data Transfer Rule (1)

Texas Sues Temu Over 'Spyware Disguised as a Shopping App'

Google Hit With Biden Rule Suits Over China-Based Data Transfers