Privacy Daily

DOJ Bulk Data Rule May Present Avenue for ECPA Claims, Lawyers Say

July 30, 2026 by Kara Thompson

Recent lawsuits may open a new avenue for plaintiffs to file Electronic Communications Privacy Act (ECPA) claims against businesses in nearly every sector that use tracking technologies on their websites, as courts grapple with whether a federal rule preventing foreign adversary access to U.S. data is a viable theory under the statute, lawyers told us recently.

The Bulk Sensitive Data (BSD) Rule, which DOJ began enforcing in April 2025 (see 2504020067), aims to avert foreign adversaries from accessing or weaponizing sensitive personal information from U.S. citizens or government data (see 2503100057). But recently, plaintiffs' attorneys have leveraged the rule to support data privacy and wiretapping claims, Epstein Becker lawyers blogged in July.

The BSD Rule "generally divides the world up into two types," said Josh Fattal, data protection lawyer at Morrison Foerster. One is data brokerage, which is a "misnomer," as it really refers to "any entity that shares data with a third party," where the third party isn't a direct data recipient. Then there are restricted transactions, which include vendor, employment, and investment agreements, he said in an interview.

Miriam Wugmeister, global chair of the data, cyber and privacy practice at the same firm, said there are many words defined in the rule "that are not the way you would typically think the word is used."

The data brokerage aspect is what most plaintiffs have been using to advance their theory of crime-tort exception under the ECPA, Fattal said. While the federal wiretapping statute contains one-party consent, which makes it difficult for plaintiffs to allege a privacy violation, the crime-tort exception holds that when a communication is intercepted for the purposes of committing a tortious or criminal act, the perpetrator can be held accountable (see 2507290069).

The "risk" of litigation is that claims are "encompassing very common activity," such as real-time bidding, "which is a major driver of the ad tech ecosystem," due to "the breadth of the data brokerage definition," he said.

In a mid-June decision, the U.S. District Court for Northern Illinois ruled that invoking the BSD Rule satisfied the ECPA crime-tort exception in *Baker v. Index Exchange* (see 2606160060).

The wiretapping litigation space has been "majorly active," and this ruling found that using the bulk data rule "is a viable theory," said Fattal. He predicted this may lead to a

rise in ECPA cases using this line of thinking to get around the federal statute's higher bar of one-party consent (see 2605050078).

The Epstein Becker lawyers specializing in privacy and healthcare issues also discussed *Christy v. Lenovo* in their blog. In that February ECPA case, the plaintiff claimed tracking technologies on the Lenovo website transmitted "persistent identifiers" of more than 100,000 U.S. citizens to the company's Chinese parent, without Lenovo implementing the security controls required by the Cybersecurity and Infrastructure Security Agency. This constitutes a violation of the rule, the plaintiff argued, and thus satisfied the crime-tort exception to the ECPA.

All Sectors Potentially Impacted

In an email to *Privacy Daily*, Epstein Becker lawyer Elena Quattrone said something "unique" about the BSD Rule is that it "affects all industry," from healthcare to retail to website providers and platforms. "Any company that's dealing with a significant amount of consumer data should be mindful of these new tactics and learn more about ways to mitigate risk," she said.

Fattal agreed. Since almost "every company and every website owner -- practically speaking -- has adtech on their website," a lot of businesses need to take steps to try and mitigate their risk, he said. Ensuring compliance with the bulk data rule is one way to go about it, including conducting "diligence" to determine if any third parties a company works with would be considered a covered person affiliated with a country of concern under the rule.

Wugmeister, however, noted that the adtech industry is a significant target of these suits.

Quattrone also said companies should "strive to comply" with the BSD Rule, as well as "understand" it "and its requirements." She added, "Compliance minimizes liability exposure under these legal theories."

Though the *Index Exchange* ruling is from a federal district court, even if it eventually gets "overruled or overturned," Fattal suspects "you could still see plaintiffs citing … this [ruling] more generally in other circuits … or in other districts."

The plaintiffs' "bar has been very active when it comes to wiretapping litigation, and so anything that opens the door" to more litigation "does pose some risk to companies, regardless of how this specific case … ultimately winds up," he added.

Remaining Questions

In the email, Quattrone's colleague Lisa Pierce Reisz added that for companies, the "significance" of these decisions is that "the BSD Rule is no longer just a regulatory statute which has its own complex web of requirements, but rather it can now be

wielded to infuse civil liability for private litigants in a variety of ways."

But there are still "lots of lingering questions" since "no court has definitively ruled on these issues yet," she added. "What will happen here is still to be determined," but people are "monitoring."

Fattal agreed. For one, "there are a number of criteria that you have to meet" to be subject to the DOJ rule, including being a U.S. person and processing a certain amount of data that falls under the rule. Additionally, the data processed must fit under one of the two types of transactions under the rule mentioned earlier. The court only ruled on part of those considerations in the *Index Exchange* case.

Examining whether the data a company processes meets the volume and type requirements covered is "an early threshold question" that needs an answer "to determine if you actually have an issue under the bulk data rule," which "wasn't really fleshed out or dived into in depth in [the *Index Exchange*] decision," said Fattal.

While there have been other cases alleging bulk data rule violations under this crime-tort exception theory, *Index Exchange* has gotten the farthest, he said.

Further, Fattal said the list of countries of concern under the rule is "not permanent" and "can be changed."

Not only could you add "countries to the list, but you could also remove countries," said Wugmeister, though she noted the rule is mostly focused on China given that it's "such a big market" that "many companies have relationships with" it.

Members of Congress have also sought clarification from the DOJ on "why certain government-related locations are and aren't on the list" of what's covered under the rule, so there's "interest also on the Hill regarding the rule," Fattal said.

Overall, "we're definitely seeing a lot of enforcement activity" and "interest in data transfers to China more generally," and this kind of litigation is "one piece of that pattern," Fattal said. He cited the Florida attorney general's foreign threats unit (see 2602130061), the FTC's enforcement of the Protecting Americans' Data from Foreign Adversaries Act (PADFAA) (see 2602190055) and action from Texas AG Ken Paxton (R) against Chinese-based companies (see 2602170040) as other examples.

Reisz agreed. "Using the BSD Rule in this way is an example of a broader theme we're seeing in private litigation whereby class action attorneys, or other private litigants, are trying to use old laws to expand liability under these new regulations," she said.