HAYNES BOONE

Federal Court Denies Motion to Dismiss Amid Alleged DOJ Bulk Data Rule Violations

By Tim Newman, Richard Weber, Brianne Wylie | July 22, 2026

RELATED PRACTICES Class Action Defense, Privacy and Cybersecurity, Technology Contracts Litigation, Litigation, White Collar and Investigations

A federal judge in Illinois recently declined to dismiss a class action complaint in part because the plaintiff had sufficiently alleged violation of the Department of Justice (DOJ)'s Bulk Data Rule. The court held the violations triggered the crime/tort exception to consent under the Federal Wiretap Act. The decision has significant implications for companies in the digital advertising, data analytics and cross-border data sharing sectors.

In *Baker v. Index Exchange Inc.*, No. 25-cv-10517 (N.D. Ill. June 16, 2026), the court denied a motion to dismiss a putative class action, finding the plaintiff adequately alleged that a supply-side advertising platform violated the Federal Wiretap Act, 18 U.S.C. § 2511, by intercepting the plaintiff's communications and transmitting his sensitive personal data to a Chinese-owned company in violation of the "Bulk Data Rule"—the DOJ regulation implementing President Biden's 2024 executive order targeted at preventing foreign adversaries from accessing U.S. government data or the sensitive personal data of Americans.

The plaintiff, John Baker, a user of BibleGateway.com, alleged that Index Exchange—a Canadian company that operates a real-time bidding platform for digital advertising—collected data about his online activity, including his IP address, cookie identifiers, advertising identifiers, and device and browser information, and shared it with Temu, an e-commerce platform and "Chinese company with substantial operations and executive oversight in the People's Republic of China." Baker alleged this conduct violated the Wiretap Act.

Index Exchange argued Baker's claims should be dismissed because BibleGateway.com had consented to Index Exchange's data collection by integrating its code into the site, thus defeating any claims under the Wiretap Act. However, the court held that the crime/tort exception applied. Baker had plausibly alleged the interception was undertaken for the purpose of committing a criminal or tortious act, namely a violation of the Bulk Data Rule's prohibition on data brokerage transactions involving sensitive personal data and "covered persons" connected to countries of concern, such as China. The court brushed aside Index Exchange's argument that the Bulk Data Rule could not apply because (1) its principal place of business is in Canada and (2) Temu's parent company, PDD Holdings, had its principal place of business in Ireland. The court found these arguments insufficient to defeat Baker's Wiretap Act claims at the pleading stage.

Three Key Takeaways Emerge from the Decision:

Private Litigation Risk is Increasing: *Baker* shows that plaintiffs' counsel are prepared to use alleged Bulk Data Rule violations as the predicate "criminal or tortious act" needed to defeat the consent defense to Wiretap Act liability under 18 U.S.C. § 2511(2)(d)—a novel interpretation and the first decision to address whether plaintiffs may rely on alleged Bulk Data Rule violations in this manner. Because the Wiretap Act authorizes statutory damages without proof of actual harm, and because this case proceeds as a putative class action, the potential financial exposure could be substantial. Companies that collect, use or share user data through advertising technology or similar tracking mechanisms should recognize that regulatory compliance failures under this rule may now translate directly into private civil liability, independent of any government enforcement action.

Cross-border Data Flows Face Greater Scrutiny: *Baker* raises the stakes for companies whose businesses depend on cross-border data flows—including advertising technology, data analytics, cloud services and business process outsourcing—given that the Bulk Data Rule restricts transfers of sensitive personal data and government-related data to “countries of concern” (currently China, including Hong Kong and Macau, Russia, Iran, North Korea, Cuba and Venezuela) or to “covered persons” connected to them. Notably, the court found that Index Exchange Inc., the Canadian parent company, could face vicarious liability for the alleged Bulk Data Rule violations of its U.S.-based subsidiary’s officers and employees, as U.S. persons directed the transaction within the scope of their employment—meaning a non-U.S. parent or affiliate structure does not, by itself, insulate a company from exposure. At the pleading stage, the court also declined to resolve whether Temu’s ownership structure placed it outside the definition of a “covered person,” leaving that factual dispute for discovery. Comparable claims are thus likely to survive into costly discovery, even where a company believes it has a strong factual defense, and the broad definition of a “data brokerage transaction” may usher in arrangements not traditionally viewed as brokerage at all.

Compliance Programs Matter More Than Ever: Considering this decision, companies should treat Bulk Data Rule compliance as a litigation risk-management priority rather than merely a regulatory checkbox. We recommend that clients take the following steps:

- Revisit data-mapping procedures to confirm they accurately reflect what sensitive personal data is collected, how it is categorized and where it ultimately flows.
- Scrutinize vendor and partner arrangements, particularly demand-side advertising partners, data integration or “cookie syncing” partners, cloud and outsourcing providers and any counterparties that could plausibly qualify as “covered persons” under the Bulk Data Rule.
- Assess data brokerage and data-sharing activities against the rule’s broad definitions, keeping in mind that arrangements not traditionally viewed as “brokerage” may nonetheless fall within its scope.
- Evaluate and strengthen controls governing transfers of sensitive personal data to confirm alignment with the rule’s restrictions, including with respect to employees and officers who are U.S. persons and who may be found to have directed a covered transaction.

The *Baker* decision is an important signal that the Bulk Data Rule is becoming a new front in private litigation, with implications reaching well beyond advertising technology and into any business that touches cross-border data flows. We encourage clients to review their data practices proactively rather than waiting for a claim to arise.