Simpson Thacher

Memorandum

Federal Court Allows Wiretap Claim to Proceed Based on Alleged DOJ Bulk Sensitive Data Rule Predicate Violation

July 7, 2026

In a first-of-its-kind pleading-stage decision, a federal district court in *Baker v. Index Exch. Inc.*, No. 25 C 10517 (N.D. Ill. June 16, 2026), denied a motion to dismiss a putative class action alleging that supply-side platform ("SSP") Index Exchange Inc. and its affiliate Index Exchange USA, LLC violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511 (the "Federal Wiretap Act"), in connection with alleged data transfers to a Chinese e-commerce platform.[1] The ruling did not determine whether the defendants, any publisher, or any advertising partner actually violated the Federal Wiretap Act or the Department of Justice bulk sensitive data ("BSD") rule. The decision is notable because the court considered whether alleged violations of the BSD rule—which prohibits or restricts certain transfers of data by U.S. persons to prescribed "countries of concern" and companies with nexus to these countries of concern—could defeat a consent defense under the Federal Wiretap Act's crime/tort exception.[2] The DOJ has designated China (including Hong Kong and Macao), Cuba, Iran, North Korea, Russia, and Venezuela as "countries of concern" based on the risk they pose of exploiting BSD to the detriment of U.S. national security. U.S. companies and their affiliates engaging in or facilitating online advertising should carefully review their vendor arrangements, data fields, consent flows, privacy notices, contractual controls, and onward transfers to identify possible transfers of website traffic information to companies with nexus to "countries of concern." The decision also highlights that companies located outside the U.S. with U.S.-based affiliates may face wiretapping claims under vicarious-liability theories where the alleged conduct is sufficiently tied to U.S.-based personnel or operations.

Index Exchange's Services in the Online Advertising Ecosystem

SSPs are one piece of the complex plumbing underlying the modern online advertising ecosystem. Index Exchange provides services to website publishers to enable real-time bidding for online advertising. According to the facts alleged in *Baker*, Index Exchange collects data about website visitors to websites that engage Index Exchange's services, bundles the data into a "bid request," transmits it to advertising partners, and delivers the winning advertiser's ad to the visitor on the website.[3] The alleged process occurs over the course of milliseconds. Index Exchange is also alleged to match website visitors with identifiers provided by third-party partners, allowing both

[1] *Baker v. Index Exch. Inc.*, No. 25 C 10517, 2026 U.S. Dist. LEXIS 133750, at 1-2 (N.D. Ill. June 16, 2026).

[2] 28 C.F.R. § 202.601; *Baker v. Index Exch. Inc.*, No. 25 C 10517, at 14.

[3] *Baker v. Index Exch. Inc.*, No. 25 C 10517, at 2-3.

companies to identify the individual. As relevant here, the plaintiff in *Baker* alleged that Index Exchange "intercepted" website traffic data and transmitted it to a Chinese e-commerce platform as part of that process.

Federal Wiretap Act Framework

The Federal Wiretap Act prohibits intentionally intercepting the contents of wire, oral, or electronic communications, and allows individuals to bring a civil claim for statutory damages of the greater of $100 per day or $10,000.[4] In Federal Wiretap Act claims, a threshold issue is whether the challenged data elements constitute the "contents" of a communication, as opposed to identifiers, routing information, device information, or other metadata-like fields. This legal analysis depends on the precise data fields transmitted—including URLs, page context, identifiers, IP addresses, device data, geolocation data, or other event data—and whether those fields reveal the contents of a communication or instead function as routing, addressing, signaling, or advertising identifiers. The statute also includes a one-party consent defense, but the availability and scope of that defense turns on whether one party to the communication validly consented to the specific interception. The consent defense, however, may be defeated if the interception was "for the purpose of committing any criminal or tortious act," which is referred to as the crime/tort exception. The scope and applicability of the crime/tort exception is subject to ongoing litigation.[5] *Baker* is notable because it addressed, at the pleading stage, whether alleged violations of the BSD rule can fall within that exception.

The Bulk Sensitive Data Rule as a Predicate Violation of the Crime/Tort Exception

The DOJ's BSD regulations generally prohibit U.S. persons from (1) knowingly entering into data brokerage transactions involving access by "covered persons" to sensitive personal data, (2) knowingly engaging in certain restricted data transactions with "covered persons" without satisfying the proscribed security requirements; and (3) knowingly directing any covered data transaction that would be a prohibited transaction if engaged in by a U.S. person. A "covered person" includes non-U.S. entities organized or principally based in or majority owned by persons who are in a "country of concern," including China.[6] The rule's application depends on the transaction type, the parties, the data categories involved, whether applicable bulk thresholds or government-related data rules are met, and whether the transaction is prohibited or instead subject to security requirements and other compliance obligations.

At the pleading stage, the Court found that the plaintiff adequately alleged a violation of the BSD rule for purposes of surviving a motion to dismiss based on the crime/tort exception. The Court did not resolve whether the website traffic data meets BSD's bulk thresholds, and it deferred the question whether the Chinese e-commerce platform meets the definition of a "covered person" as a factual dispute not appropriate for resolution on a motion to dismiss. The Court also found that Index Exchange Inc., a Canadian company, could be held liable for the alleged

[4] 18 U.S.C.S. § 2520.

[5] *Goulart v. Cape Cod Healthcare, Inc.*, No. 25-10445-RGS, 2025 U.S. Dist. LEXIS 119435 (D. Mass. June 24, 2025), appeal docketed, No. 25-1672 (1st Cir. July 23, 2025).

[6] 28 CFR § 202.601.

BSD violations of the employees and officers of its U.S.-based subsidiary under a theory of vicarious liability. Key issues remain unresolved, including whether the specific data fields at issue are sensitive personal data that meet the applicable bulk thresholds, whether the recipient qualifies as a covered person, whether the alleged bid-request disclosures constitute interception of contents, whether any consent defense applies, and whether the facts ultimately support vicarious liability.

Practical Steps

Recommended steps include mapping bid-request fields and identifier-syncing flows; identifying publishers, exchanges, demand-side platforms, resellers, and other advertising partners that may receive or onward-transfer data; screening relevant recipients for country-of-concern or covered-person risk; documenting whether sensitive-data categories and thresholds are implicated; reviewing user-facing disclosures and consent flows; updating contractual restrictions on onward transfers; and implementing technical controls to block, segment, or restrict prohibited or high-risk data flows. For publishers in sensitive verticals, including health, financial, children's, location-based, or other sensitive-content environments, companies should separately assess whether bid-request fields, page URLs, taxonomy labels, or identifiers reveal sensitive information that may trigger heightened federal, state, or contractual restrictions.

For further information regarding this memorandum, please contact one of the following authors:

WASHINGTON, D.C.

Abram J. Ellis
+1-202-636-5579
aellis@stblaw.com

LOS ANGELES

Kim T. Le
+1-310-407-7551
kim.le@stblaw.com

NEW YORK CITY

George S. Wang
+1-212-455-2228
gwang@stblaw.com

Alexander J. Franchilli
+1-212-455-6654
alexander.franchilli@stblaw.com

Shuhao Fan
+1-212-455-3036
shuhao.fan@stblaw.com