IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JOHN BAKER,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	**Case No. 25 C 10517**
	)	
INDEX EXCHANGE INC. and	)	
INDEX EXCHANGE USA, LLC,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

MATTHEW F. KENNELLY, District Judge:

John Baker has brought a putative class action lawsuit against Index Exchange Inc. and Index Exchange USA, LLC. Mr. Baker alleges that the defendants violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511, by intercepting his communications with BibleGateway.com and transmitting his sensitive personal data to Temu, a Chinese-owned company. The defendants have moved to dismiss Baker's first amended complaint. For the reasons below, the Court denies the defendants' motion to dismiss.

Background

The following facts are taken from the complaint's factual allegations and this case's procedural history.

Index Exchange is a supply-side platform (SSP) that facilitates the sale of ad space on websites by transmitting information about web users and the content they are viewing to digital advertisers through real-time bidding auctions. When a user visits a participating website, Index Exchange automatically transmits data about the user to its

many advertising partners, often called demand-side partners, who may be interested in showing the user an ad. The data shared includes details about the webpage and identifiers unique to the user, including IP address, cookie data, and advertising IDs. This data also includes inferred information about the user's device, location, demographics, interests, browsing behavior, and content the user is viewing. Index Exchange bundles this data in a transmission called a "bid request" and transmits the bid request to demand-side partners. Index Exchange's demand-side partners use the information they receive in a bid request to decide how much they are willing to pay to target a particular individual with an ad. Index Exchange then processes the bids, enabling the participating website to sell the ad placement to the highest bidder. The process takes just milliseconds. Index Exchange's demand-side partners receive this data through bid requests for every eligible United States user who visits a website that contracts with Index Exchange to participate in its ad sale process.

In addition to transmitting data through bid requests, Index Exchange maintains direct data integrations with other companies. Through these data integrations, Index Exchange shares the behavioral and device-level data that it has collected from website users with the other companies. This direct integration includes a separate process known as "cookie syncing" to enhance the ability of those companies to identify and track users. During this process, Index Exchange matches its internal user ID with identifiers used by companies like Temu, a Chinese-owned e-commerce platform. In response, Temu sets or retrieves its own identifier, enabling both companies to link the same individual across each of their tracking systems. These data exchanges occur in real time.

Baker, an Illinois resident, used his desktop web browser to visit BibleGateway.com, a website that participates in Index Exchange's ad sale process. Index Exchange monitored Baker's activity and intercepted his communications when he visited BibleGateway.com. Index Exchange also collected Baker's IP address, cookie IDs, browsers and device data, advertising IDs, and other behavioral information. Index Exchange shared Baker's information with other companies, including Temu, through the "cookie sync" process.

Baker filed his first amended complaint in November 2025 asserting one claim for violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511, commonly referred to as the Federal Wiretap Act.

The defendants have moved to dismiss Baker's first amended complaint under Federal Rules of Civil Procedure 12(b)(2) and 12(b)(6). The Court permitted limited jurisdictional discovery, and the parties submitted supplemental briefs based on that discovery.

Discussion

A. Rule 12(b)(2)

"A complaint need not include facts alleging personal jurisdiction." *Purdue Rsch. Found. v. Sanofi-Synthelabo, S.A.*, 338 F.3d 773, 782 (7th Cir. 2003) (cleaned up). Once a defendant moves to dismiss under Rule 12(b)(2), however, "the plaintiff bears the burden of demonstrating the existence of jurisdiction." *Id.* When ruling based on written materials alone, without the benefit of an evidentiary hearing, the plaintiff is required only to make out a *prima facie* case of personal jurisdiction. *Id.* In determining whether a *prima facie* case has been established, the Court "take[s] the plaintiff's

asserted facts as true and resolve[s] any factual disputes in its favor." *NBA Props., Inc. v. HANWJH*, 46 F.4th 614, 620 (7th Cir. 2022) (quoting *uBID, Inc. v. GoDaddy Grp., Inc.*, 623 F.3d 421, 423–24 (7th Cir. 2010)). A court may also consider affidavits on the issue of personal jurisdiction. *Id.* "[B]oth parties' affidavits are accepted as true, and where they conflict, the plaintiff is entitled to resolution in its favor." *Id.*

A court may have either general or specific personal jurisdiction over a party. *See Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 592 U.S. 351, 358 (2021). General jurisdiction exists "only when a defendant is 'essentially at home' in the State." *Id.* (citation omitted). Specific jurisdiction, on the other hand, requires that the defendant "take some act by which it purposefully avails itself of the privilege of conducting activities within the forum State." *Id.* at 359 (cleaned up). The Seventh Circuit has articulated the following test for determining whether a district court has specific personal jurisdiction over a defendant:

> Specific personal jurisdiction requires that (1) the defendant has purposefully directed his activities at the forum state or purposefully availed himself of the privilege of conducting business in the state; (2) the alleged injury arises out of or relates to the defendant's forum-related activities; and (3) any exercise of personal jurisdiction must comport with traditional notions of fair play and substantial justice.

Rogers v. City of Hobart, 996 F.3d 812, 819 (7th Cir. 2021).

As amended, Illinois's long-arm statute contains a catchall provision stating that a court "may . . . exercise jurisdiction on any other basis now or hereafter permitted by the Illinois Constitution and the Constitution of the United States." 735 ILCS 5/2-209(c). Because Illinois's long-arm statute is co-extensive with the limits of due process, the Court must find that each defendant has established minimum contacts with the forum such that it may be haled into court in this forum. "The proper focus of the 'minimum

contacts' inquiry in intentional-tort cases is 'the relationship among the defendant, the forum, and the litigation.'" *Walden v. Fiore*, 571 U.S. 277, 291 (2014) (quoting *Calder v. Jones*, 465 U.S. 783, 788 (1984)).

All parties agree that the defendants are not subject to general jurisdiction. Therefore, the Court will address only whether the Court has specific jurisdiction over the defendants.

The defendants no longer contest purposeful availment. Defs.' Supp. Reply at 2. They focus instead on arguing that the defendants' contacts with Illinois are not related to Baker's claim and that it is not fair for the Court to exercise jurisdiction over them.

The defendants acknowledge that "a strict causal relationship between the defendant's forum contacts and the claim[] in the case is not required to establish specific jurisdiction." Defs.' Supp. Reply at 4 (citing *Ford*, 592 U.S. at 362). They attempt to distinguish *Ford* by arguing that Baker's claim that he was injured based on the transfer of data to a Chinese-owned company is not related to their commercial contracts with Illinois-based publishers and advertisers. This argument, in the Court's view, takes an overly narrow view of the defendants' Illinois contacts.

According to Baker, an ad is displayed on participating websites after a bid request is accepted by one of Index Exchange's demand-side partners. The bid request transmits data about the website user to those demand-side partners before an ad may be displayed. This means, for each of the multiple-billion ad impressions that were displayed in Illinois,[1] Index Exchange must have first transmitted the data of an

[1] The Court has left out the exact figure because it is contained only in material that the Court placed under seal.

individual who was in Illinois to its demand-side partners via a bid request. Baker also alleges that Index Exchange transmitted this personal data to other partners, such as Temu, via a "cookie sync." In other words, Index Exchange intercepted and transmitted personal data of individuals located in Illinois billions of times within a one-year period as part of its real-time bidding process. Baker, an Illinois resident, alleges that as part of this process, Index Exchange intercepted and shared his data with Temu. The Court thus concludes that Baker's claims are sufficiently related to the defendants' Illinois contacts to support specific jurisdiction.

On the question of fairness, the defendants argue that it is unfair to require them to litigate in Illinois "based on the mere fact that [Baker] happened to be in Illinois when he visited BibleGateway.com . . . ." Defs.' Supp. Reply at 6. The defendants contend that this would subject them to jurisdiction in every state where its website publisher customers receive visitors. But the fact that a defendant *may* be subject to jurisdiction in many states does not make it unfair to exercise jurisdiction in a given state when the defendant has purposefully availed itself "of the privilege of conducting activities within [that] State." *Id.* (quoting *Hanson v. Denckla*, 357 U.S. 235, 253 (1958)). This was equally true for Ford even though it is a global auto company with "business everywhere." *Id.* at 355. Jurisdictional discovery revealed that Index Exchange's real time bidding process delivered billions of ad impressions to website visitors located in Illinois in just one year. Index Exchange received the location data for these users and therefore knew they were located in Illinois. Based on the significant number of ad impressions presented in Illinois, the defendants "must reasonably anticipate being hailed into" Illinois courts to defend actions based on the actions related to their real-

time bidding process. *Ford*, 592 U.S. at 364 (quoting *Keeton v. Hustler Magazine, Inc.*, 465 U.S. 770, 781 (1984)).

B. Rule 12(b)(6)

The defendants next argue that Baker's complaint must be dismissed under Rule 12(b)(6) for failure to state a claim. Under Rule 8(a), "[a] pleading that states a claim for relief must contain . . . a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). That pleading standard requires the plaintiff to allege factual material that, if taken as true, suffices to "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–57, 570 (2007). A claim is plausible on its face when the facts alleged "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Put differently, the "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555.

Rule 12(b)(6) permits a defendant to challenge whether a complaint meets this standard before filing a responsive pleading. Fed. R. Civ. P. 12(b)(6). In ruling on a Rule 12(b)(6) motion to dismiss, a court is limited to assessing the allegations in the complaint, documents attached to the complaint, documents critical to the complaint and referred to in it, and information subject to proper judicial notice. *Wertymer v. Walmart, Inc.*, 142 F.4th 491, 498 (7th Cir. 2025).

The defendants argue that Baker fails to sufficiently plead a violation of the Federal Wiretap Act. According to Baker, Index Exchange intentionally intercepted Baker's communications and data when he visited BibleGateway.com. Am. Compl. ¶ 72. Baker also alleges that Index Exchange disclosed his personal data to Temu in

violation of the Department of Justice's bulk sensitive data (BSD) regulations. Am. Compl. ¶¶ 78–91.

Subsection 2511(1)(a) of the Wiretap Act makes it unlawful for "any person" to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). It defines the "contents" of a communication to "include[] any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

Given the expansive definition of "intercept," subsection 2511(1) in isolation could reach a wide array of ordinary conduct. Subsection 2511(2) prevents those kinds of unintended results by carving out several exemptions. Of particular relevance in this case, subsection 2511(2)(d) states:

> It shall not be unlawful under this chapter for a person . . . to intercept a . . . communication . . . where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

Id. § 2511(2)(d). This exemption provides a one-party consent defense: an interception is not unlawful if at least one party gave prior consent. That defense, in turn, is subject to a crime/tort exception: if the communication was "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," the interception is unlawful notwithstanding any prior consent. *Id.*

Index Exchange contends that BibleGateway.com, a party to the communication with Baker, consented to Index Exchange's interception of the communication. Thus, the defendants argue, subsection 2511(2)(d) exempts them from liability, and the Court should dismiss Baker's complaint.

This argument first faces a potential procedural obstacle. The defendants filed a motion to dismiss for failure to state a claim, which tests the sufficiency of the plaintiff's complaint. But consent under the Wiretap Act is an affirmative defense, and a plaintiff need not anticipate or refute potential affirmative defenses in his complaint. *Doe v. Smith*, 429 F.3d 706, 709 (7th Cir. 2005). Instead, a defendant seeking dismissal based on an affirmative defense generally should raise that defense in a responsive pleading, then file a motion under Rule 12(c) for judgment on the pleadings. *Luna Vanegas v. Signet Builders, Inc.*, 46 F.4th 636, 640 (7th Cir. 2022). That distinction is necessary to correctly allocate the burdens of pleading and proof and to ensure that a plaintiff has notice of an affirmative defense and a fair opportunity to contest it. *See Gunn v. Cont'l Cas. Co.*, 968 F.3d 802, 806 (7th Cir. 2020).

There is, however, "a narrow and pragmatic exception" to the general rule against Rule 12(b)(6) dismissals based on affirmative defenses, which applies in the rare situation when a plaintiff pleads himself out of court. *Id.* "[I]f the affirmative defense is clear from the face of the complaint [and other materials properly considered on a Rule 12(b)(6) motion], the court may dismiss under Rule 12(b)(6) instead" of Rule 12(c). *Holmes v. Marion Cnty. Sheriff's Off.*, 141 F.4th 818, 822 (7th Cir. 2025).

In his response, Baker does not contest the defendants' consent defense. The Court concludes that the consent defense is clear from the face of Baker's complaint, so

it can properly serve as a basis for dismissal under Rule 12(b)(6).

Having found that the motion clears this procedural hurdle, the Court will next address the defendants' substantive arguments. As indicated, the Wiretap Act's consent defense is limited by a crime/tort exception. *See Doe*, 429 F.3d at 709. Even when consent is uncontested, as it is here, dismissal is inappropriate without considering whether Baker has plausibly pleaded that the crime/tort exception applies. *See id.* at 710. Turning to that question, Baker alleges that the crime/tort exception applies because Index Exchange violated the BSD regulations.

In February 2024, President Biden promulgated an executive order to prevent access to Americans' sensitive personal data by foreign adversaries. *See* Exec. Order No. 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, 89 Fed. Reg. 15421 (Feb. 28, 2024). The Order was issued pursuant to the President's powers under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701, and other authorities not relevant here. *Id.* The executive order directed the DOJ to enact regulations addressing the "continuing effort of certain countries of concern to access Americans' sensitive personal data . . . ." *Id.*

Based on this order, the DOJ promulgated the BSD regulations, effective April 8, 2025. The regulations prohibit U.S. persons from entering into data brokerage transactions with a "covered person" that involves access to personal sensitive data. 28 C.F.R. § 202.301. A U.S. person is "any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under

the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States." 28 C.F.R. § 202.256. The regulations also prohibit any U.S. person from knowingly directing any covered data transaction that would be a prohibited transaction if engaged in by a U.S. person. 28 C.F.R. § 202.305. A "covered person" includes a non-U.S. entity that is organized or has its principal place of business in a country of concern or is more than 50 percent owned by a country of concern or covered persons. 28 C.F.R. § 202.211. China is a country of concern. 28 C.F.R. § 202.601(a). The IEEPA and BSD regulations specify criminal and civil penalties for violations. 50 U.S.C. § 1705; 28 C.F.R. § 202.1301.

The defendants argue that the crime/tort exception does not apply because the DOJ's BSD regulations do not apply to Index Exchange, a Canadian company. The defendants also dispute Baker's allegations that Temu is a covered person under the regulations. Baker responds that the exception applies because Index Exchange is vicariously liable for its U.S. based employees' conduct and directly liable because Index Exchange USA, a corporation organized under the laws of Michigan, is Index Exchange's alter ego. Baker also contends that he has sufficiently alleged that Temu is a covered person.

Baker's invocation of vicarious liability relies on a body of case law applicable to tort actions. The Seventh Circuit has explained that the legislature has "defined tort actions 'as actions based on damage or injury from a *wrongful* or negligent act.'" *United States v. Cent. Soya, Inc.*, 697 F.2d 165, 168 (7th Cir. 1982) (quoting S. Rep. No. 1328, 89th Cong., 2d Sess.). In the context of a civil cause of action brought by the United States under the Rivers and Harbors Act, the court explained that "the government's

suit for damages against the *in-rem* defendant can only be considered an action arising from a wrongful act[.]" *Id.* This conclusion was supported by the fact that the action was "based upon the occurrence of a statutorily defined wrongful act." *Id.* Any action for damages under the Act was therefore "founded upon a tort." *Id.* at 169.

This analysis is instructive. A civil action for damages under the Wiretap Act premised upon violations of the BSD regulations is based on the alleged wrongful act of transmitting Americans' sensitive personal data in a manner that may give foreign adversaries access to such data—in other words, a wrongful act as defined in the BSD regulations. Thus the Court concludes that an action for damages under the BSD regulations is a tort action.

For tort actions, "[i]t is well established that traditional vicarious liability rules ordinarily make principals or employers vicariously liable for acts of their agents or employees in the scope of their authority or employment." *Meyer v. Holley*, 537 U.S. 280, 285 (2003). Where Congress has not expressed a contrary intent, the Supreme Court has drawn the inference that ordinary vicarious liability rules apply. *Id.* at 287. The IEEPA and BSD regulations do not limit traditional vicarious liability rules. Thus liability attributable to an entity's employee or agent is imputed to the entity.

Baker alleges that Index Exchange's CEO and other high-ranking officers are based in New York. Am. Compl. ¶ 80. Baker also alleges that "these U.S.-based members of Index Exchange Inc.'s management team acted within the scope of their employment and within the control of Index Exchange Inc. to direct the operation of Index Exchange Inc.'s [real time bidding] platform and associated data collection sharing, including with covered persons like Temu." *Id.* The defendants argue that this

is a conclusory allegation that is insufficient because it does not offer any specific transaction, date, communication, approval process, or decision by a U.S. based officer. But the defendants do not contend that any heightened pleading standard that would require these additional details applies to Baker's claim.

Furthermore, as an entity, Index Exchange can only act through its officers and employees. Baker includes additional detailed allegations about Index Exchange's collection of Baker's sensitive personal data and transmission of that data, as part of a bulk data transaction, with Temu. Am. Compl. ¶¶ 78–91. These actions must have been taken by Index Exchange's officers and employees.

As noted, the BSD regulations prohibit any U.S. person from knowingly directing any data transaction that would be prohibited if engaged by a U.S. person. 28 C.F.R. § 202.305. Based on this provision, it appears to the Court that an action undertaken by a U.S.-based employee—a U.S. person—of a non-U.S. corporation can violate the BSD regulations if the U.S.-based employee knowingly directs a prohibited data transaction.

The Court concludes that Baker sufficiently alleges that Index Exchange's U.S.-based employees and officers—who are U.S. persons covered by the BSD regulations—violated the BSD regulations by directing bulk data transactions with Temu. The Court further concludes Index Exchange may be liable for its U.S.-based employees and officers alleged violations of the BSD regulations based on traditional vicarious liability rules.

Baker's alter ego argument does not fare as well. Baker argues that Index Exchange is directly liable for violation of the BSD regulations because Index Exchange USA, a U.S. entity, acts as Index Exchange's alter ego. As Baker notes, the state of

incorporation typically provides the substantive rule for alter ego claims. *Wachovia Sec., LLC v. Banco Panamericano, Inc.*, 674 F.3d 743, 751 (7th Cir. 2012). Index Exchange USA is incorporated in Michigan, so the Court will apply Michigan law.

Under Michigan law, a parent corporation is liable for the actions of its subsidiary when the subsidiary is acting as the "alter ego" of the parent. *Green v. Ziegelman*, 310 Mich. App. 436, 452 (2015). A plaintiff must plead the following elements for alter ego liability: (1) the entity is a mere instrumentality of its owner; (2) the entity was used to commit fraud or wrongdoing; and (3) misuse of the entity caused an unjust loss to the plaintiff. *Id.*

Baker's complaint fails to plead the second element. He alleges that Index Exchange, the parent company, collected his data and transmitted it to Temu in violation of the BSD regulations. Baker does not allege that Index Exchange USA committed fraud or wrongdoing or that it was established to facilitate fraud or wrongdoing. The Court therefore concludes that Baker has not sufficiently pleaded that Index Exchange USA is Index Exchange's alter ego for purposes of establishing the parent company's liability for violating the BSD regulations.[2]

The defendants also argue that the BSD regulations do not apply to them because Baker has not sufficiently alleged that Temu is a "covered person." Baker alleges that "Temu qualifies as a 'covered person' under 28 C.F.R. § 202.211(a) because it is operated and controlled by PDD Holdings Inc., a Chinese company with substantial operations and executive oversight in the People's Republic of China—a

[2] The Court need not address the impact of this conclusion on whether Baker has sufficiently pleaded a claim against Index Exchange USA because that entity does not independently seek dismissal.

'country of concern' under the BSD Rule." Am. Compl. ¶ 81. The defendants argue that Temu is not a covered person because PDD has its principal executive offices in Ireland, and publicly available records show that Temu's U.S. operations are conducted through Whaleco, Inc., a U.S. registered and headquartered company. This boils down to a factual dispute that is not appropriate for resolution at this stage. The Court concludes that Baker's allegations are sufficient to support a contention that Temu is a covered person under the BSD regulations.

To summarize, even if BibleGateway.com consented to the interception of its communications with Baker, he has sufficiently alleged that the crime/tort exception applies based on Index Exchange's alleged violation of the BSD regulations. The Court therefore concludes that Baker has stated a claim under the Electronic Communications Privacy Act, 18 U.S.C. § 2511.

Conclusion

For the above reasons, the Court denies the defendants' motion to dismiss Baker's first amended complaint [dkt. no. 29]. The parties are directed to confer regarding a discovery and pretrial schedule and are directed to file a joint status report with a proposed schedule by June 23, 2026. The telephonic status hearing set for July 14, 2026 is vacated and advanced to June 30, 2026 at 8:55 a.m., using call-in number 650-479-3207, access code 2305-915-8729.

Date: June 16, 2026

MATTHEW F. KENNELLY
United States District Judge