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

JOHN BAKER, individually and on behalf of all others similarly situated, *Plaintiff*, v. INDEX EXCHANGE, INC., *Defendant*.	Case No.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff John Baker ("Plaintiff") brings this Class Action Complaint and Demand for Jury Trial on behalf of himself and all others similarly situated against Index Exchange, Inc. ("Index Exchange" or "Defendant") for unlawfully intercepting users' online communications and transmitting their sensitive data to a Chinese-owned entity, in violation of federal privacy and national security laws. Plaintiff alleges as follows based on personal knowledge as to himself and on information and belief as to all other matters.

NATURE OF THE ACTION

1. This case arises from a dangerous and unlawful data-sharing arrangement between a Canada-based advertising platform that conducts extensive business in the United States and a foreign adversary of the United States. Defendant Index Exchange knowingly and systematically transmitted sensitive user data intercepted from U.S. websites to Temu, an e-commerce platform owned and operated by a Chinese-founded parent company with deep ties to China and widely reported links to its intelligence apparatus.

2. In April 2025, the U.S. Department of Justice implemented the Data Security

Program, a national security initiative codified at 28 C.F.R. Part 202 (the "Bulk Sensitive Data Rule" or "BSD Rule") pursuant to Executive Order 14117.

3. The BSD Rule prohibits transferring in bulk the sensitive personal data of Americans to persons or entities tied to "countries of concern," including China, to prevent adversarial countries from acquiring data that can be used to surveil, exploit, or model U.S. consumer behavior.

4. As a senior Justice Department official explained, the BSD Rule aims to stop foreign governments from sidestepping American cybersecurity protections entirely: "[W]hy would you go through the trouble of complicated cyber intrusions and theft to get Americans' data when you can just buy it on the open market or force a company under your jurisdiction to give you access? . . . The [BSD Rule] makes getting that data a lot harder."

5. The BSD Rule makes clear that it is unlawful for advertising platforms to send Americans' personal data to Chinese companies through automated tracking and targeting systems. The Justice Department has explained that this includes sharing identifiers and behavioral information with platforms linked to foreign governments. That is precisely the kind of data-sharing misconduct at issue in this case.

6. In direct violation of the BSD Rule, Index Exchange, through its automated advertising infrastructure, transmits U.S. user data to Temu—a Chinese-owned e-commerce platform. Temu receives this data in real time as part of its participation in Index Exchange's ad delivery system.

7. Temu has come under increasing scrutiny from regulators and members of Congress over concerns that its data practices may facilitate surveillance by the Chinese government. Investigators have even warned that Temu may operate as a conduit for state-

directed data collection targeting U.S. residents.

8. As of June 2025, Index Exchange maintained direct integrations with Temu, enabling the company to bid on advertising inventory and receive behavioral and device-level data from U.S. consumers' online activities. These transmissions fall squarely within the BSD Rule's definition of bulk sensitive personal data and are expressly prohibited.

9. Index Exchange had ample notice that its conduct was unlawful. It participates in industry associations that engaged directly with the BSD Rule rulemaking process and publicly warned members of the legal risks of transmitting behavioral data to entities based in China. Index Exchange even helped create the very technology that enables the type of data sharing explicitly addressed by the BSD Rule.

10. Index Exchange's conduct gives rise to claims under the Electronic Communications Privacy Act ("ECPA" or "Wiretap Act"), 18 U.S.C. § 2510 *et seq.,* because Index Exchange intentionally intercepted consumers' communications with the intention of disclosing that data in furtherance of a criminal or tortious act: specifically, the unlawful transmission of U.S. consumers' bulk sensitive personal data to a prohibited foreign entity in violation of the BSD Rule.

11. This case raises urgent questions at the intersection of privacy, commercial surveillance, and national security. The U.S. government has determined that the export of Americans' sensitive data to hostile foreign regimes constitutes an "unusual and extraordinary threat . . . to the national security and foreign policy of the United States that has been repeatedly recognized across political parties and by all three branches of government."[1] Index Exchange

[1] *Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries,* U.S. DOJ (Apr. 11, 2025),

ignored that warning. It must now be held accountable.

12. Plaintiff Baker's sensitive and private information was unlawfully intercepted and then shared by Index Exchange with Temu. He seeks statutory damages under the ECPA as well as equitable relief, including an injunction barring Index Exchange from continuing its unlawful data transfers to entities affiliated with foreign adversaries.

PARTIES

13. Plaintiff John Baker is a natural person and citizen of Evanston, Illinois.

14. Defendant Index Exchange is a corporation organized and existing under the laws of Canada, with its principal place of business in the United States located at 3WTC 175 Greenwich St., 39th Floor, New York, New York 10007.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because cases under the ECPA, 18 U.S.C. § 2510 *et seq*., raise a federal question and pursuant to 28 U.S.C. § 1332(d)(2) because (i) at least one member of the Class is a citizen of a different state than any Defendant, (ii) there are more than 100 members of the Class, (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (iv) none of the exceptions under that subsection apply to this action.

16. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District.

17. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial part of the

---

https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive (internal quotation omitted).

events or omissions giving rise to Plaintiff's claims occurred in the District.

COMMON FACTUAL ALLEGATIONS

I. Index Exchange Exposes Americans' Sensitive Data to Foreign Adversaries.

18. In the world of digital advertising, Index Exchange is known as a supply-side platform ("SSP").

19. As an SSP, Index Exchange facilitates the sale of ad space by transmitting information about web users and the content they are viewing to advertisers through real-time bidding ("RTB") auctions. When a user visits a participating website or app, Index Exchange automatically transmits a set of data to its many advertising partners, often called "demand-side partners," who may wish to show the user an ad. This data includes details about the webpage, identifiers unique to that user (such as IP address, cookie data, and advertising IDs), and inferred information about the user's device, location, demographics, interests, browsing behavior, and the content the user is viewing—including the webpage's full URL. This information is bundled up and shared by Index Exchange with its demand-side partners in a transmission called a "bid request."

20. A bid request informs potential advertisers or their intermediaries about the opportunity to show an ad to the user and invites them to submit bids to serve an advertisement in that ad slot. By sharing this extensive data in the bid request, Index Exchange increases the value of the ad slot by enabling advertisers to better predict whether the user will click on the ad or make a purchase. This dynamic incentivizes Index Exchange to collect and share highly detailed information about the user.

21. To make the ad slot as appealing as possible, Index Exchange includes a trove of in-depth information about the user and the content they're viewing in the bid request it sends out. In addition to data collected directly from the user's browser or device, the bid

request may also contain behavioral or demographic "segments." These are predefined categories that describe the user's likely interests, characteristics, or conditions—allowing advertisers to target individuals with extreme precision.

22. Via its website, Index Exchange offers its customers "off-the-shelf and customi[z]able Inventory Packages designed for [the customer's] marketing KPIs [key performance indicators] or seasonal campaigns. Options include: **Full funnel**—build campaigns according to your marketing goal[;] **Streaming TV**—targeted content and creative formats at scale[;] **Seasonal campaigns**—curate supply for the year's biggest marketing events." (Emphasis in original).

23. Index Exchange facilitates the placement of users into segments based on a wide variety of inferred user traits, ranging from a user's geographical location or hobbies to the user's religion, mental health, or anticipated interest in shopping at Black-owned or women-owned businesses.

24. Demand-side partners use the information they receive from Index Exchange's bid request—including persistent user identifiers, page content, and segment data—to decide how much they are willing to pay to target a particular individual. These identifiers are not just for matching ads; they are often shared with or compared against third-party datasets and data brokers to further expand the user's profile. The richer and more specific that profile becomes, the more precisely the user can be targeted.

25. Index Exchange then processes these bids, enabling the website owner or app developer to sell the ad placement to the highest bidder for maximum financial return. The entire process takes just milliseconds, and involves Index Exchange, the participating bidders, and potentially other identity services, all set in motion by Index Exchange's bid request and

powered by the information it collects about the website, the user, and the user's behavior. This process is not performed for just a handful of users—Index Exchange's demand-side partners receive this data through bid requests for every eligible U.S. user who visits a website that uses Index Exchange's technology.

26. In addition to transmitting data through the bid request, Index Exchange also initiates a separate process known as "cookie syncing" with certain advertising partners to enhance the ability of those partners to identify and track the user even more effectively. During this "cookie sync," Index Exchange matches its own internal user ID with identifiers used by third parties like the Chinese-owned e-commerce platform Temu. To do this, it directs the user's browser to contact Temu-owned server endpoints—such as temu.com/api/adx/cm/pixel-index—passing Index Exchange's user ID to Temu in the request.

27. In response, Temu sets or retrieves its own identifier, enabling both companies to link the same individual across their separate tracking systems. These data exchanges occur in real time and without meaningful notice to, or consent from, the user.

28. When a partner like Temu receives this data from Index Exchange, it can combine it with its own tracking tools—such as pixel identifiers and post-click analytics—to construct a far more detailed and invasive picture of the user. From a single ad impression, Temu can infer the user's location, device type, browsing environment, and the exact content the user is viewing—including how they engage with it through clicks, hovers, or time spent. Over time, these data points allow Temu to assemble a persistent and evolving digital dossier that tracks the user's behavior across websites, sessions, and contexts—without their knowledge or consent.

29. In this role, Temu functions not only as an advertiser but also as a real-time analytics and profiling engine—collecting users' behavioral signals to refine targeting, optimize

ad delivery, and build detailed profiles of U.S. consumers, including across sensitive content categories.

30. For example, if a user frequently visits articles about debt consolidation, pregnancy, or job hunting, and clicks on finance-related headlines, Temu could infer that the user is experiencing financial distress or is planning for a family. These insights may then be used to personalize e-commerce listings, promote low-cost or sensitive products, or optimize ad strategies to exploit perceived vulnerabilities or needs. Critically, the user is never notified that this profiling is occurring, or that their behavioral data is being shared with a company linked to a foreign intelligence apparatus.

31. In the hands of a foreign adversary, this detailed data can serve purposes far beyond e-commerce. A platform like Temu, operating under Chinese jurisdiction, can use this real-time behavioral data to build detailed dossiers on U.S. residents, uncover psychological or financial vulnerabilities, and identify individuals in sensitive roles—such as military personnel, journalists, judges, or dissidents. This data can be weaponized for profiling, coercive targeting, or even blackmail, all without the user ever knowing that their information is being transmitted to a foreign-controlled entity. Indeed, such vulnerabilities prompted the passage of the BSD Rule.

32. Index Exchange's role in this ecosystem is central and intentional. It distributes and maintains the tracking code, collects the data, syncs identifiers with third parties, and broadcasts bid requests containing that data to downstream recipients—including foreign advertisers. Rather than take reasonable steps to minimize or reduce the sharing of such personal information, Index Exchange's platform is specifically designed to maximize the commercial

value of user data by enabling downstream recipients like Temu to act on it in real time, regardless of the geopolitical or security risks.

II. The BSD Rule Prohibits the Transmission of This Data to Entities Like Temu.

33. On April 8, 2025, the U.S. Department of Justice implemented the Data Security Program, codified at 28 C.F.R. Part 202, to restrict the transfer of bulk sensitive data to "countries of concern," including China. Under the BSD Rule, it is unlawful to transfer "bulk U.S. sensitive personal data"—including persistent identifiers—to "covered persons" under the control of adversarial foreign governments. 28 C.F.R. § 202.101(a).

34. Temu has been widely condemned as a national security threat. In 2023, Google delisted an app owned by Temu's parent company after detecting malware that exploited device vulnerabilities to exfiltrate user data.[2] In 2024, twenty-one state attorneys general issued a formal warning about Temu's invasive data practices and its legal obligations under Chinese law to cooperate with state intelligence agencies.[3] And in 2025, the attorneys general of Nebraska and Kentucky filed lawsuits against Temu, alleging that its mobile app functions as spyware.[4] [5]

---

[2] Brian Krebs, *Google Suspends Chinese E-Commerce App Pinduoduo Over Malware,* Krebs on Security (Mar. 22, 2023), https://krebsonsecurity.com/2023/03/google-suspends-chinese-e-commerce-app-pinduoduo-over-malware/.

[3] Letter from A. Knudsen, Mont. Att'y Gen., et al., to Mr. Qin Sun, President of Temu, et al. (Aug. 15, 2024), https://files.constantcontact.com/d3e83e11901/268c1faf-83b5-425e-90b2-bf34fa9921e9.pdf.

[4] *Attorney General Hilgers Files Lawsuit Against Temu for Siphoning Nebraskans' Phone Data,* Neb. Att'y Gen. (June 12, 2025), https://ago.nebraska.gov/news/attorney-general-hilgers-files-lawsuit-against-temu-siphoning-nebraskans-phone-data.

[5] Erin Ross, *Kentucky attorney general sues Temu for allegedly stealing data,* LEX 18 (last updated Jul. 21, 2025 2:22 PM), https://www.lex18.com/news/covering-kentucky/attorney-general-coleman-files-lawsuit-against-temu-for-alleged-kentucky-brand-personal-data-theft.

35. Through its integration with Index Exchange, Temu covertly obtains and processes sensitive data about millions of Americans as they browse websites related to health, reproductive care, financial distress, mental health, and other deeply personal topics.

36. Index Exchange facilitates these transfers by transmitting protected identifiers to Temu in real time. These identifiers enable Temu to track, profile, and target Americans based on their private interests and vulnerabilities. This unlawful data flow gives a foreign adversary the ability to silently surveil U.S. residents in violation of the BSD Rule.

37. Index Exchange has knowingly continued routing Americans' sensitive user data to Temu well after the BSD Rule came into effect.

III. Index Exchange Has Knowingly Violated the BSD Rule.

38. Index Exchange is not a naïve participant in the digital advertising ecosystem. It is a member of multiple industry organizations—including the Network Advertising Initiative (NAI)—that submitted formal comment letters to the DOJ during the BSD Rule's rulemaking process.[6] These comments specifically warned that behavioral tracking, cookie syncing, and cross-border integrations with demand-side platforms could run afoul of the Rule if foreign adversaries were involved.

39. Index Exchange is deeply familiar with the technology at the heart of the data sharing in this case. In 2011, Index Exchange co-authored the OpenRTB specification, a protocol that enables the programmatic buying and selling of digital ad space. OpenRTB standardized how supply-side platforms like Index Exchange communicate with demand-side players, and it

[6] *NAI Comments on DOJ Rulemaking on Data Brokerage and Bulk Sensitive Data,* NAI (Dec. 2, 2024), https://thenai.org/nai-comments-on-doj-rulemaking-on-data-brokerage-and-bulk-sensitive-data/.

remains the foundation of real-time bidding today. Index Exchange cannot claim ignorance of the data flows involved here—it helped design them.

40. Despite its knowledge of the BSD Rule's requirements, Index Exchange continued to transmit U.S. user data to Temu through its advertising system. This included unique identifiers, browsing activity, and contextual information about the pages users visited—all collected and shared in real time without users' knowledge. Index Exchange's infrastructure enabled Temu to track and profile Americans as they engaged with a wide range of websites, including those covering sensitive and personal topics.

41. Index Exchange's conduct was not accidental or peripheral—it was done knowingly and intentionally and is core to its business model. Its integration with Temu reflects an intentional business decision made in disregard of a federal rule adopted to address an "unusual and extraordinary threat" to the national security of the United States.

FACTS SPECIFIC TO PLAINTIFF

42. In the time since the BSD Rule came into effect, Plaintiff John Baker has used his desktop web browser to visit BibleGateway.com, a website offering access to scripture, analysis, and religious study resources.

43. Plaintiff Baker visited BibleGateway.com to read scripture and engage with the other religious content on the site.

44. As soon as Plaintiff Baker accessed the site, he was unknowingly being observed and tracked by Index Exchange. While Plaintiff browsed, Index Exchange was covertly monitoring his activity and intercepting his communications with the website.

45. Without Baker's knowledge or consent, Index Exchange intercepted the full URLs of the webpages Plaintiff visited on BibleGateway.com. These URLs reveal what he was

reading—disclosing not just that he visited a religious site but the very passages he was exploring and what he may have been seeking guidance on. Additionally, Index Exchange also surreptitiously collected Plaintiff's IP address, cookie IDs, browser and device data, advertising IDs, and behavioral information.

46. Index Exchange packaged the data it had collected about Baker and initiated the real-time bidding process described above, sharing Plaintiff's sensitive data with Index Exchange's demand partners.

47. This was not the end of Index Exchange's use of Baker's data as Index Exchange also enabled the de-anonymization of Plaintiff's information by initiating a "cookie sync" with its third-party advertising partners.

48. Temu was one such advertising partner. That is, through its integration on BibleGateway.com and related websites, Index Exchange directed Plaintiff's browser to contact server endpoints owned by Temu. Once that contact was established, Index Exchange shared with Temu the user ID it had associated with Plaintiff.

49. By sharing Plaintiff's user ID with Temu, Index Exchange gave and transmitted to Temu the information needed to associate Plaintiff with the data held in Temu's tracking system. Index Exchange's activity empowered third parties, like Temu, to construct an ever-more-detailed profile on Plaintiff Baker, giving these entities the ability to persistently track Plaintiff across multiple websites.

50. Prior to Index Exchange's collection and sharing of Plaintiff's sensitive data, he was not informed that Index Exchange was integrated into BibleGateway.com. Plaintiff was also unaware that visiting BibleGateway.com would result in Index Exchange sharing his personal

information—including sensitive data about the religious content he was viewing—with third parties including Temu.

51. Plaintiff did not consent to Index Exchange's collection of his data and did not consent to the sharing of his data with third parties, including third parties like Temu who are subject to the control of an adversarial country.

52. Despite Plaintiff's lack of knowledge or consent, Index Exchange intercepted Plaintiff's communications and sensitive personal data, packaged his personal data for sale, and violated the BSD Rule by unlawfully sharing that sensitive data with Temu, an entity associated with a country of concern.

53. Plaintiff was harmed by this unlawful interception. By intercepting his communications for the purpose of violating the BSD Rule, Index Exchange undermined Plaintiff's ability to control his sensitive personal information and private religious interests and protect that information from persons identified by the U.S. as threats to national security and the safety of U.S. citizens.

CLASS ACTION ALLEGATIONS

54. **Class Definitions**: Plaintiff John Baker brings this proposed class action pursuant to Federal Rule of Civil Procedure 23(b)(2) and Rule 23(b)(3) on behalf of himself and a Class (collectively the "Class") of all others similarly situated, defined as follows:

> **Class**: All individuals in the United States whose electronic communications with websites incorporating Index Exchange's tracking technology were intercepted and whose personal data—including persistent identifiers and behavioral activity—was transmitted to Temu or other entities based in China on or after April 10, 2025.

Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors,

predecessors, and any entity in which Defendant or its parents have a controlling interest and its officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

55. **Numerosity**: The exact number of Class members is unknown and not available to Plaintiff at this time, but individual joinder is impracticable. On information and belief, Defendant has many thousands of users who fall into the definition of the Class. Class members can be identified through Defendant's records.

56. **Commonality and Predominance**: There are questions of law and fact common to the claims of Plaintiff and the putative Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

(a) Whether Defendant used tracking technologies to cause users' web browsers to reroute electronic communications—including URLs, metadata, and behavioral activity—to Defendant and to Temu;

(b) Whether Defendant used a device, as defined under 18 U.S.C. § 2510(5), to intercept the contents of communications from Plaintiff and the Class;

(c) Whether Defendant obtained valid consent from Plaintiff and the Class to intercept and disclose their electronic communications to third parties, including foreign entities;

(d) Whether the data transmitted by Defendant constitutes "bulk U.S. sensitive personal data" under the BSD Rule;

(e) Whether Defendant's transmission of that data to Temu constitutes a prohibited data brokerage transaction under the BSD Rule;

(f) Whether Defendant acted knowingly and with intent to share the information; and

(g) Whether Defendant's interception and disclosure of users' communications falls within the crime-tort exception to the ECPA's party-consent provision.

57. **Typicality**: Plaintiff's claims are typical of the claims of members of the Class in that Plaintiff, like all members of the Class, had his information unlawfully intercepted and has been injured by Defendant's misconduct at issue.

58. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff and the members of the Class sustained injuries and damages as a result of Defendant's conduct. Plaintiff also has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel has any conflicts with or interests adverse to the Class.

59. **Superiority**: Class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, as joinder of all members of the Class is impracticable. Individual litigation would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer

management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, expense and uniformity will be fostered and enhanced.

60. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definitions" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violation of Electronic Communications Privacy Act ("ECPA")
18 U.S.C. § 2510, *et seq*.
(On behalf of Plaintiff and the Class)

61. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

62. The ECPA prohibits any person from "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

63. **Intentional Interception**: Defendant Index Exchange intentionally distributes and maintains tracking scripts, pixels, and header bidding infrastructure on third-party websites that reroute user communications, including Plaintiff and the Class's communications, to Index Exchange's own servers and those of third parties. Index Exchange's technologies capture the contents of Plaintiff's and its other users' interactions with these websites and transmit them to Index Exchange and its integrated demand-side partners, including foreign buyers.

64. Index Exchange's tracking code executed automatically within Plaintiff's and Class members' browser during the page load process. This code intercepted the contents of Plaintiff's and Class members' interactions with those websites by rerouting first-party communications—including full URLs, page titles, and a taxonomical classification of the content of the page—to Index Exchange and other third parties. These interceptions occurred as part of the browser's rendering sequence, before Plaintiff or members of the Class could detect,

review, or prevent the transmissions.

65. As users like Plaintiff and members of the Class navigate websites such as BibleGateway.com, Index Exchange's JavaScript code causes their browsers to transmit full URLs, page titles, and other page-level metadata to Index Exchange's servers in real time. These transmissions occur without the user's awareness or consent and are initiated automatically during the same browser session in which the user communicates with the website. Index Exchange's capture of these communications constitutes an unlawful interception under the ECPA.

66. **Contents of a Communication**: The data intercepted by Index Exchange from Plaintiff Baker and the Class includes full-page URLs. These qualify as the "contents" of a communication under 18 U.S.C. § 2510(8) because they reveal the substance and subject matter of Plaintiff's and the other users' communications with the host website.

67. **Use of a Device**: The technologies Index Exchange uses to intercept this data—including JavaScript, tracking pixels, and header bidding scripts—constitute "devices" under 18 U.S.C. § 2510(5), which includes any device or apparatus used to intercept electronic communications.

68. **Lack of Consent**: Plaintiff's and the Class members' communications and data were shared surreptitiously and without their consent. Index Exchange did not provide clear or conspicuous notice that user interactions with websites would be surveilled and routed to foreign entities, and Plaintiff and Class members lack a reasonable means to detect, prevent, or opt out of Index Exchange's data collection and sharing. There was no actual or implied consent under applicable law.

69. **Crime-Tort Exception**: Even if Index Exchange were deemed a party to these

communications, which it is not, the "party exception" in 18 U.S.C. § 2511(2)(d) does not apply. At the time of the interception, Index Exchange's interception and use of these communications was undertaken knowingly and intentionally for the purpose of committing a criminal and tortious act—namely, the unlawful transmission of bulk U.S. sensitive personal data to a covered foreign entity in violation of the BSD Rule, 28 C.F.R. Part 202.

70. On or after April 8, 2025, Index Exchange knowingly engaged in prohibited data-brokerage transactions with Temu, a foreign-owned entity with its principal place of business in China, in violation of the BSD Rule. 28 C.F.R. § 202.301(a).

71. Index Exchange is a corporation organized and existing under the laws of Canada, with its principal place of business located in the State of New York. Because Index Exchange is a person in the United States, Index Exchange is a "U.S. person" under 28 C.F.R. § 202.256.

72. 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 "country of concern" under the BSD Rule. Although PDD Holdings nominally lists its principal executive offices in Ireland, it maintains a significant presence in China and is subject to Chinese law, including China's National Intelligence Law, Cybersecurity Law, and Data Security Law. These laws compel Chinese companies and individuals to secretly cooperate with government surveillance efforts and grant authorities unrestricted access to private user data. Temu's operations are therefore presumptively subject to Chinese government control, oversight, and compelled disclosure obligations.

73. Index Exchange initiates synchronization requests with Temu infrastructure—including requests to URLs such as temu.com/api/adx/cm/pixel-index—which result in the

transmission of numerous protected "listed identifiers" under the BSD Rule, including but not limited to IP addresses (28 C.F.R. § 202.234(g)), advertising IDs (28 C.F.R. § 202.234(e)), device IDs (28 C.F.R. § 202.234(c)), and cookie data (28 C.F.R. § 202.234(g)).

74. Index Exchange transmits these protected identifiers together, including, for example, transmitting a given user's IP address along with the user's device ID, such that the identifiers are clearly linked with one another and are associated or reasonably capable of being associated with each related user.

75. Index Exchange failed to take reasonable steps to minimize this communication and data sharing with prohibited covered entities. Indeed, as described throughout this pleading, its system was designed to do largely the opposite.

76. This information qualifies as "covered personal identifiers" and "sensitive personal data" under the BSD Rule because these identifiers are shared with Temu 1) in combination with at least one other listed identifier, or 2) in combination with other data such that the listed identifier is or can reasonably be associated with other listed identifiers or other sensitive personal data. 28 C.F.R. §§ 202.212(a), 202.249(a).

77. On information and belief, Index Exchange has collected or maintained this sensitive personal data relating to Plaintiff and more than 100,000 other U.S. persons (including Plaintiff and Class members) following the effective date of the BSD Rule, and therefore this information constitutes "bulk U.S. sensitive data" under 28 C.F.R. § 202.206.

78. On information and belief, Index Exchange has provided this bulk U.S. sensitive data regarding Plaintiff and the Class to Temu as part of transactions between the two entities. Temu itself did not collect or process this data directly from Plaintiff and the Class, and Index Exchange's provision of this bulk U.S. sensitive data to Temu, a covered person, constitutes a

"covered data transaction involving data brokerage" under 28 C.F.R. §§ 202.210 and 202.214(b)(4)-(9).

79. Index Exchange is aware of this conduct and the BSD Rule. It is a sophisticated entity in the digital advertising industry. Not only does Index Exchange maintain a specialized internal regulatory compliance team, it is a member of multiple industry associations that directly participated in the BSD Rule rulemaking process and publicly warned members of the legal risks of transmitting certain data to entities based in China.

80. Index Exchange even co-founded the Interactive Advertising Bureau (IAB) TechLab, a group that specializes in creating industry standards for advertising technology like real-time bidding, which is at the core of the conduct addressed by the BSD Rule. Index Exchange knew or reasonably should have known that it had engaged and was engaging in covered data transactions involving data brokerage in violation of the BSD Rule.

81. Because Index Exchange knowingly engaged and engages in covered data transactions involving data brokerage of Plaintiff's and the Class members' communications and data with Temu, a covered person, Index Exchange has violated the BSD Rule's prohibition of data-brokerage transactions under 28 C.F.R. § 202.301(a).

82. Index Exchange intentionally and knowingly intercepted and disclosed Plaintiff's and Class members' communications and data to Temu and related entities for the purpose of committing this criminal and tortious act. As such, it is not shielded by the "party exception" under the ECPA.

83. Plaintiff and the Class suffered harm as a result of Defendant's violations of the ECPA, including the transmission of their sensitive data to a foreign adversary identified as a threat to national security and the safety of U.S. citizens. Plaintiff and the Class therefore seek

(a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(c)(2), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff John Baker individually and on behalf of the Class, prays for the following relief:

(a) An order certifying the Class as defined above, appointing John Baker as the representative of the Class, and appointing his counsel as Class Counsel;

(b) An order declaring that Defendant's actions, as set out above, violate the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*.;

(c) An injunction requiring Defendant to cease all unlawful activities;

(d) An award of statutory damages, disgorgement of profits, punitive damages, costs, and attorneys' fees;

(e) Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully submitted,

Dated: September 2, 2025

By: /s/ *Michael Ovca*

Michael Ovca
movca@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Counsel for Plaintiff and the Putative Class