Brandt Silverkorn (SBN 323530)
bsilverkorn@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Alleged Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

MARISSA PORCUNA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

XANDR, INC., a Delaware corporation,

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR

(1) Violation of 18 U.S.C. § 2510, *et seq.*;
(2) Invasion of Privacy; and
(3) Intrusion Upon Seclusion.

AND DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Marissa Porcuna ("Plaintiff") brings this Class Action Complaint and Demand for Jury Trial on behalf of herself and all others similarly situated against Xandr, Inc. ("Xandr" 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 herself 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 U.S.-based advertising platform and a foreign adversary of the United States. Defendant Xandr, Inc., a Microsoft subsidiary, knowingly and systematically transmitted sensitive user data intercepted from U.S. websites to Temu, a Chinese e-commerce platform, which has been the subject of widespread reports linking it to China's state 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 (hereafter referred to as the "Bulk Sensitive Data Rule" or "BSD Rule") pursuant to Executive Order 14117. The BSD Rule prohibits transferring, in bulk, the sensitive personal data of Americans to 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. As a senior Justice Department official explained, the 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."

3. The BSD Rule makes clear that sending consumers' information to Chinese advertising platforms through automated ad systems is prohibited. The examples provided by DOJ—including advertising systems transmitting identifiers and behavioral data to covered entities—mirror the types of data flows at issue in this case.

4. In direct violation of the BSD Rule, Xandr, through its automated advertising infrastructure, transmits Plaintiff's and potentially millions of other U.S. consumers' data to Temu.

5. Temu has come under increasing scrutiny from regulators and members of Congress over concerns that its data practices facilitate surveillance by the Chinese government. Investigators have warned that Temu functions as a conduit for state-directed data collection targeting U.S. residents.

6. Xandr transmits behavioral "segment data" to Temu that reflect the interests, routines, and potential vulnerabilities of U.S. consumers. When Plaintiff visited a website to read about diabetes, Xandr intercepted and disclosed the full page context, health-related segments, and persistent identifiers to Temu. This transmission enabled Temu to link Plaintiff's browsing activity to her identity, track her behavior across the web, and build detailed profiles reflecting Plaintiff's health status and other private attributes.

7. In the hands of a foreign adversary, this data can be used to assemble detailed behavioral profiles, identify psychological or financial weaknesses, and monitor individuals in sensitive roles—such as journalists, judges, or military personnel. These capabilities pose not only a profound invasion of privacy but also a direct threat to national security, including the risk of coercion, reputational harm, or blackmail.

8. Xandr had ample notice that its conduct was unlawful. It is a member of industry groups that participated in the BSD Rule rulemaking and publicly warned that behavioral tracking and data flows to entities in China could violate the law.

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

10. 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' behavioral data to hostile foreign regimes or entities under their jurisdiction 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] Xandr ignored that warning. It must now be held accountable.

11. Plaintiff seeks statutory damages under the ECPA as well as equitable relief, including an injunction prohibiting Xandr from continuing its unlawful bulk data transfers to entities affiliated with foreign adversaries.

PARTIES

12. Plaintiff Marissa Porcuna is a natural person and citizen of the State of California. She resides in Bay Point, which is located within the Northern District of California.

13. Defendant Xandr, Inc. is a corporation organized and existing under the laws of Delaware, with its principal place of business located at One Microsoft Way, Redmond, Washington 98052.

JURISDICTION AND VENUE

14. 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 the Class Action Fairness Act, 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.

[1] *Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries,* U.S. DOJ (Apr. 11, 2025), https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive (internal quotation omitted).

15. 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.

16. Venue is proper pursuant to 28 U.S.C. § 1391(b) because Plaintiff resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District.

DIVISIONAL ASSIGNMENT

17. Pursuant to Northern District of California Civil Local Rules 3-2(c), 3-2(d), and 3-5(b), assignment to the Oakland Division is proper because a substantial part of the events giving rise to the Plaintiff's claims occurred in Contra Costa County, and Plaintiff resides in Contra Costa County.

COMMON FACTUAL ALLEGATIONS

I. Xandr Exposes Americans' Behavioral Data to Foreign Adversaries.

18. Xandr Inc. operates one of the most sophisticated surveillance and targeting systems in the global advertising industry. Formerly known as AppNexus—and now a wholly owned subsidiary of Microsoft Corporation—Xandr functions as a programmatic advertising exchange embedded across thousands of high-traffic websites and mobile applications.

19. Xandr participates in this system as both a demand-side and supply-side platform. That means that on one end, it provides tools that allow advertisers to bid for ad space across the web. On the other end, it integrates with publishers (e.g., website operators and mobile app developers) by operating a variety of data collection technologies into their websites and apps, including:

- JavaScript trackers, which are small snippets of code embedded in web pages to monitor user activity, such as which pages are viewed, for how long, and what links are clicked;

- Prebid.js adapters, which are bits of code that allow websites to auction their ad space to multiple advertisers simultaneously before the page finishes loading; and
- Cookie-syncing endpoints, which instruct the user's browser to contact third-party servers and share identifiers, allowing different adtech companies to recognize and track the same user across multiple sites and devices.

20. Using these technologies, Xandr intercepts data directly from users' browsers while they are actively browsing the web. When a user visits a website with Xandr's tracking infrastructure—such as Plaintiff visiting diabetesforum.com—Xandr captures and transmits a detailed snapshot of that user's online session in what's called a "bid request."

21. The bid request transmitted by Xandr includes persistent identifiers such as cookie IDs, device IDs, mobile advertising IDs, and IP address, along with device metadata like screen resolution, browser version, operating system, and language settings. It also captures contextual information, including the full URL of the visited page and its referring source. This contextual data reveals the specific contents of what the user is viewing—such as articles, forum posts, or other sensitive material—at the moment the data is broadcast to bidders.

22. Beyond this, Xandr supplements the request with dozens of identifiers from third-party tracking companies through a process called cookie syncing. This involves instructing the user's browser to contact other tracking domains and exchange unique IDs. These shared identifiers allow Xandr and its partners to recognize the same user across different websites. This identity linkage is what enables long-term tracking—even across sites that the user has never directly interacted with.

23. Xandr does not merely transmit identifiers or metadata in isolation. It enriches this data with behavioral segments, which are labels that describe the user's inferred interests, demographics, and circumstances based on prior browsing activity, location patterns, or third-party data overlays. These segments can reveal, for example, whether a user appears to be interested in cancer treatment, debt relief, addiction recovery, or political causes. The segments are transmitted alongside identifying information, giving downstream recipients a highly detailed snapshot of the user's behavior and private traits.

24. As introduced above, one of the downstream recipients of this sensitive data is Temu, a Chinese e-commerce platform owned by PDD Holdings Inc. When Temu participates in a real-time bidding ("RTB") auction through Xandr's exchange, it receives the behavioral segment labels, identifiers, and page context associated with the user.

25. This enables Temu to not only decide whether to serve an ad but also to retain and analyze the data for future targeting. As a result, even if Temu has never tracked the user before, it can connect the data received from Xandr—including browsing activity and behavioral segments—to its own records, enabling persistent cross-site profiling.

26. In the example above, Plaintiff's visit to diabetesforum.com triggers the assignment of health-related segments. These segments, such as "Chronic Condition > Diabetes," or more granular health classifications assigned by partners—are sent as part of the bid request. Even if the user is not logged in, Xandr's partnerships with identity providers and its use of shared identifiers allow it to link that activity to a broader profile of the user across other websites and browsing sessions.

27. These behavioral segments can include intensely sensitive classifications. Depending on the user's browsing behavior and the segment provider, they may reflect traits such as:

- "Job Role > Legal - Judge"
- "Incest/Abuse Support"
- "Her2 Positive – Breast Cancer"
- "Made a Charitable Donation - Conservative Politics"
- "Gambling Addiction"
- "Liberal Views on LGBTQ Rights and Pro-Choice"
- "Occupation > Disabled"

28. The segments are not anonymized. They are linked to persistent identifiers that allow for long-term tracking and enrichment across contexts. The transmission of this data is also not limited to the winning bidder. As regulators and technologists have observed, Xandr's RTB system broadcasts bid requests to all eligible bidders—including foreign platforms like Temu—many of whom retain the data even if they do not win the auction. This exposure occurs invisibly and automatically, without any direct interaction from the user.

29. In the hands of a foreign adversary, this data can be used for more than just 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, identify psychological or financial vulnerabilities, and target 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's knowledge that their information is being transmitted to a foreign-controlled entity. Indeed, such vulnerabilities prompted the passage of the BSD Rule.

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

30. On April 8, 2025, the U.S. Department of Justice issued the BSD Rule, codified at 28 C.F.R. Part 202, to restrict the transfer of Americans' bulk sensitive personal data to "countries of concern," including China. Under the BSD Rule, it is

unlawful to transfer "bulk U.S. sensitive personal data"—including the categories of persistent identifiers that Temu obtains from Xandr—to certain entities associated with adversarial foreign governments.

31. 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 Chinese 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]

32. Through cookie syncing and real-time bid requests facilitated by Xandr, 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.

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

III. Xandr Has Knowingly Violated the BSD Rule.

34. Xandr is not a passive or uninformed actor in the digital advertising ecosystem. It is a member of multiple industry groups—including the Network Advertising Initiative (NAI)—that actively participated in the rulemaking process

---

[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://www.tn.gov/content/dam/tn/attorneygeneral/documents/pr/2024/temu-letter.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.

leading to the U.S. Department of Justice's adoption of the Bulk Sensitive Data Rule ("BSD Rule") in April 2025. In public comment letters submitted to DOJ, these trade associations specifically warned that common adtech practices—such as behavioral profiling, cookie syncing, and real-time bidding with foreign demand-side platforms—could violate the BSD Rule if data was transmitted to entities linked to foreign adversaries like China.

35. Xandr's awareness of this legal risk is further reflected in corporate disclosures. In Microsoft's 2024 Annual Report (Form 10-K), the company warned investors that its advertising operations are subject to rapidly evolving privacy and data transfer regulations, including cross-border restrictions that could materially impact business operations. As a Microsoft subsidiary, Xandr is subject to centralized legal oversight, and its business practices are shaped by shared infrastructure, policies, and contractual standards across Microsoft's advertising ecosystem.

36. In the wake of the BSD Rule's implementation, Microsoft amended its partner contracts to include explicit representations and warranties regarding compliance. For example, Microsoft now requires its partners to certify that they are not "covered persons" under the BSD Rule and to refrain from engaging in "covered data transactions" involving bulk U.S. sensitive personal data or government-related data.

37. However, the mere inclusion of this clause in Microsoft's boilerplate advertising agreement is legally and operationally insufficient. It does nothing to prevent violations where Microsoft or Xandr themselves initiate the bulk data transfers or continue integrations with known covered entities. Under the BSD Rule, liability is not limited to the covered recipient, it extends to any U.S. company that transmits restricted data to them.

38. Despite the DOJ's clear guidance and Microsoft's updated contractual language, Xandr has continued to transmit sensitive user data to Temu, a Chinese-

owned platform operating under the jurisdiction of a foreign adversary. These transmissions include persistent identifiers, browsing behavior, and contextual metadata—such as the URLs of health-related websites—that enable Temu to track, profile, and retain data about U.S. residents in real time.

39. Xandr's conduct is not accidental, peripheral, or the result of isolated technical missteps. By maintaining active integrations with Temu, Xandr knowingly facilitated the export of Americans' behavioral data to a foreign adversary. In doing so, it disregarded binding federal law, the BSD Rule, created specifically to address what the U.S. government has called an "unusual and extraordinary threat" to the national security and foreign policy of the United States.

FACTS SPECIFIC TO PLAINTIFF PORCUNA

40. Plaintiff Marissa Porcuna is a resident of California. Following a medical diagnosis in 2013, Plaintiff Porcuna regularly uses the Internet to research personal health topics and access support communities. In June 2025, Plaintiff Porcuna visited the website diabetesforum.com, a health-focused forum where users discuss chronic illness, medical treatments, and related concerns.

41. Plaintiff Porcuna was independently subjected to the same conduct by Xandr. While Plaintiff was actively viewing pages on these websites, her browser loaded JavaScript code operated by Xandr. This code triggered an identity sync to de-anonymize the users' data across multiple identity providers and initiated automated bid requests sent from Plaintiff's browser to Xandr's servers. Those bid requests featured persistent identifiers uniquely associated with Plaintiff—including her cookie IDs, device IDs, IP addresses, and browser metadata—along with the full URL of the specific health-related page that Plaintiff was viewing at the time.

42. Xandr then enriches this bid request with other data before sending it to purchasers of ad inventory. Bid requests of this form standardly include behavioral segment data, which further indicate Plaintiff's health interests and vulnerabilities,

even beyond what is revealed by the URL itself. These segments, together with the page-level context, were broadcast to dozens of adtech entities participating in Xandr's real-time bidding auction—including Temu, a Chinese-owned platform operating under the jurisdiction of a foreign adversary. As a result, Temu received detailed information about Plaintiff's online behavior and health-related interests in real time, without their knowledge or consent.

43. Xandr's covert tracking and sharing of Plaintiff's sensitive data violates her reasonable expectation of privacy. This data, particularly when appended to persistent profiles, reveals intimate details about Plaintiff. Aggregating and monetizing this information without Plaintiff's knowledge or consent goes far beyond what any reasonable consumer would expect and constitutes a serious intrusion into private life.

44. Plaintiff did not consent to the interception, enrichment, or foreign transmission of her browsing data. Xandr's conduct caused Plaintiff concrete and particularized harm, including the unauthorized disclosure of sensitive personal information to a foreign entity, the invasion of her privacy, and the loss of control over how and where her health-related behavior was shared and used.

CLASS ACTION ALLEGATIONS

45. **Class and Subclass Definitions**: Plaintiff Marissa Porcuna brings this proposed class action pursuant to Federal Rule of Civil Procedure 23(b)(2) and Rule 23(b)(3) on behalf of herself and a Class ("Class") and subclass ("California Subclass") of all others similarly situated, defined as follows:

> **Class**: All individuals in the United States whose electronic communications with websites incorporating Xandr'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.

California Subclass: All members of the Class who resided in the State of California at the time their electronic communications with websites incorporating Xandr's tracking technology were intercepted and transmitted to Temu or other entities based in China.

Excluded from the Class and Subclass 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.

46. **Numerosity**: The exact number of Class and Subclass 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 and Subclass. Class and Subclass members can be identified through Defendant's records.

47. **Commonality and Predominance**: There are questions of law and fact common to the claims of Plaintiff and the alleged Class and Subclass, and those questions predominate over any questions that may affect individual members of the Class or Subclass. Common questions for the Class and Subclass members 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;

(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;

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

(h) For the California Subclass, whether Defendant's conduct violated the California Constitution or intruded upon the privacy rights of California residents.

48. **Typicality**: Plaintiff's claims are typical of the claims of members of the Class and Subclass. The claims arise from a common nucleus of operative fact—inter alia, the surreptitious interception and illicit transfer of their personal information to a foreign adversary of the United States. Plaintiff Porcuna, like all members of the Class and Subclass, had her information unlawfully intercepted and has been injured by Defendant's misconduct at issue.

49. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and Subclass and has retained counsel

competent and experienced in complex litigation and class actions. Plaintiff's claims are representative of the claims of the other members of the Class and Subclass. That is, Plaintiff and the members of the Class and Subclass sustained injuries and damages as a result of Defendant's conduct. Plaintiff also has no interests antagonistic to those of the Class or Subclass, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and Subclass and have the financial resources to do so. Neither Plaintiff nor their counsel have any conflicts with or interests adverse to the Class or Subclass.

50. **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 and Subclass 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 as well as the risk of inconsistent adjudication. 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. Through a class action, economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

51. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class and Subclass Definition" 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)

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

53. 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).

54. **Intentional Interception**: Defendant Xandr knowingly and intentionally distributes and maintains and uses tracking scripts, pixels, and header bidding infrastructure on third-party websites for the purpose of rerouting user communications to Xandr's own servers and those of third parties. Xandr's technologies intentionally capture the contents of users' interactions with these websites and purposefully transmit them to Xandr and its integrated demand-side partners, including foreign buyers. Xandr's tracking code—JavaScript embedded in the source code of partner websites—executed automatically within Plaintiff's and Class members' browsers 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 Xandr 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.

55. As users like Plaintiff and members of the Class navigate websites such as diabetesforum.com, Xandr's JavaScript code causes their browsers to transmit full URLs, page titles, and other page-level metadata to Xandr'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. Xandr's capture of these communications constitutes an unlawful interception under the ECPA.

56. **Contents of a Communication**: The data intercepted by Xandr from Plaintiff Porcuna and members of 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 the user's communications with the host website.

57. **Use of a Device**: The technologies Xandr 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.

58. **Lack of Consent**: Plaintiff and Class members did not consent to Xandr's interception or disclosure of their communications. Xandr did not provide clear or conspicuous notice that user interactions with publisher 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 Xandr's data collection and sharing. There was no actual or implied consent under applicable law.

59. **Crime-Tort Exception**: Even if Xandr 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, Xandr'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.

60. On or after April 8, 2025, Xandr 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).

61. Xandr is a corporation organized and existing under the laws of Delaware, with its principal place of business located in the State of Washington. Because Xandr, Inc. is organized under the laws of the United States and is an entity in the United States, Xandr is a "U.S. person" under 28 C.F.R. § 202.256.

62. 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 subject to Chinese government control, oversight, and compelled disclosure obligations.

63. Xandr initiates synchronization requests with Temu infrastructure—including requests to URLs such as https://temu.com/api/adx/cm/pixel-xandr—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)), and cookie data (28 C.F.R. § 202.234(g)).

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

65. While the above already represents a significant violation of user privacy, on information and belief, the full scope of user data that Defendant transmits to Temu—enabled through standard identifiers in real-time bidding—goes well beyond what an end user can directly observe. On information and belief, server-to-server communications between Xandr and Temu transmit information such as device IDs (28 C.F.R. § 202.234(c)), user behavioral signals, and a multitude of other advertising identifiers, all made available to Temu to further refine its consumer profiles.

66. 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).

67. On information and belief, Xandr has collected or maintained this sensitive personal data relating to more than 100,000 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.

68. On information and belief, Xandr provides this information to Temu as part of commercial transactions between the two entities. Temu itself did not collect or process this data directly from the relevant individuals, and Xandr'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, 202.214, and 202.214(b)(4)-(9).

69. Xandr is a sophisticated entity in the digital advertising industry. It is a member of 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. Xandr also acknowledged in its own SEC filings that it actively monitors privacy and data transfer regulations. For these reasons, Xandr 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.

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

71. In addition to Xandr's tortious and criminal intent to violate the BSD Rule by sharing certain information with Temu and potentially other entities subject to the jurisdictional control of China, as described further below, the aforementioned interception by Xandr was also knowingly and intentionally performed for the independent purpose of committing tortious acts in violation of California common law, specifically:

a. Violating Plaintiff's and the California Subclass members' right to privacy conferred by the California Constitution through the creation and dissemination of highly detailed identity profiles, enriched by the contents of Plaintiff's and the California Subclass members' communications intercepted by Xandr, as described herein; and

b. Committing the tort of intrusion upon seclusion under California common law by using the contents of the intercepted communications to facilitate the creation of highly detailed identity profiles on Plaintiff and Class members, which were then used and disseminated as described herein.

72. Because Xandr intentionally and knowingly intercepted and disclosed Plaintiff's and Class and Subclass members' communications for the purpose of committing these criminal and tortious acts, it is not shielded by the "party exception" under the ECPA.

73. 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, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and disgorgement of 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.

SECOND CAUSE OF ACTION

Invasion of Privacy Under the California Constitution (On behalf of Plaintiff and the California Subclass)

74. Plaintiff and the California Subclass members incorporate the foregoing allegations as if fully set forth herein.

75. Article I, section one of the California Constitution guarantees to every California citizen the inalienable right to privacy.

76. In keeping with this right, Plaintiff and the California Subclass members have a legally protected interest in preventing the unauthorized collection, aggregation, and dissemination of their most personal information, particularly when this data reflects sensitive aspects of their personal lives like their private health conditions. Plaintiff and the California Subclass also have a strong interest in preventing the widespread distribution of detailed behavioral profiles to unknown third parties—including foreign entities—without their knowledge or consent

77. These individuals maintain a reasonable expectation of privacy in their day-to-day lives—an expectation that extends not only to their Internet browsing activity and online communications, but also to the personal data that Xandr surreptitiously collects, enriches, de-anonymizes, and sells without the knowledge or consent of Plaintiff and the California Subclass members.

78. Xandr intentionally invades these interests, violating Plaintiff's and the California Subclass members' reasonable expectation of privacy through its covert collection, aggregation, correlation, and dissemination of sensitive information and persistent identifiers tied to Plaintiff and the California Subclass members as alleged herein.

79. Xandr's technology is designed to collect, analyze, monetize and share sensitive consumer data for targeted advertising and user profiling. Xandr conducts real-time surveillance of users engaging with deeply personal content—such as

online support groups for private health conditions—capturing a broad array of sensitive data. Xandr intentionally and extensively violates the reasonable expectation of privacy held by Plaintiff and the California Subclass members through engaging in this covert, large-scale data collection, designed to uniquely identify and surveil individuals. This extensive covert surveillance and targeting would be highly offensive to a reasonable person and constitutes an egregious breach of social norms.

80. Xandr secretly harvests and correlates personal information, enriches that data with additional details, and builds highly detailed identity profiles unique to each individual. These enriched profiles are then shared with potentially thousands of undisclosed third parties, including entities under the control of adverse foreign governments, for profit through the RTB process. These unknown third parties are then empowered to target individuals based on sensitive behavior and inferred characteristics.

81. Xandr does not merely collect isolated data points from Plaintiff and the California Subclass members. It stockpiles a vast range of personal information, including persistent identifiers (e.g., cookie IDs, device IDs, mobile advertising IDs, and IP addresses), device metadata (e.g., screen resolution, browser version, operating system, and language settings), and contextual information such as full URLs and referring pages. This contextual data often reveals the exact content being viewed by the individual at the very moment Xandr broadcasts the data to bidders.

82. Through these practices, Xandr intercepts, tracks, collects, aggregates, and redistributes the Internet activity and communications of Plaintiff and the California Subclass. Xandr's cookie-syncing processes further enable the linkage of user identifiers across websites, facilitating persistent cross-site tracking and user recognition, allowing Xandr to link activity across websites and sessions, building a detailed, persistent profile on each individual.

83. By combining its central role in the RTB ecosystem with technologies

like JavaScript trackers, Prebid.js adapters, and cookie-syncing endpoints, Xandr compiles and constantly refines a previously unimaginable record of the attributes, Internet activity, and communications of Plaintiff and California Subclass members.

84. This widespread surveillance and distribution of personal data occurs without meaningful disclosure and defies users' reasonable expectations of privacy. No reasonable user would expect that a company like Xandr—a company most consumers have never heard of—would collect and distribute sensitive information about their physical and mental health concerns to a vast network of unknown companies.

85. Xandr exploits this vast trove of data to create or assign segments to users—classifications that allow Xandr and its downstream partners to categorize each user in a highly granular manner. These detailed segments are not based only on demographic information but may also be based on deeply sensitive attributes like mental or physical health conditions, financial distress, disability, and religious beliefs.

86. These segments are shared alongside uniquely identifying information, providing not just a detailed snapshot of the user's traits but the ability to permanently tie those traits to an infinitely expandable and re-shareable dossier on that individual. Xandr shares these profiles, including detailed segment data, with potentially thousands of unknown third parties. The information is distributed in real time and may also be retained by these downstream partners, creating additional copies of these dossiers that can be used, enhanced, and re-shared indefinitely. By facilitating this process, Xandr not only violates Plaintiff's and the California Subclass members' reasonable expectation of privacy but also empowers downstream entities to do the same.

87. Secretly collecting such data in sensitive contexts is highly offensive. Correlating that information into detailed user profiles, then enabling advertisers and

data brokers to tie those profiles to real-world identities, is highly offensive. Sharing those profiles—containing behavioral and potentially identifying data—with a global network of bidders for profit is highly offensive.

88. Among the third parties receiving this sensitive data is Temu, a foreign-owned company with its principal place of business in China. When Temu participates in an RTB auction through Xandr's exchange, it receives behavioral segment data, persistent identifiers, and the context of the web page being viewed. This allows Temu not only to serve targeted ads but also to retain and analyze that information for future use, thereby gaining deep visibility into users' habits, interests, and vulnerabilities.

89. As described above, the U.S. government has identified China and its control of personal data as adversarial to national security and the safety of U.S. citizens. Americans have a strong interest in protecting their personal data from an entity the U.S. government has identified as a threat to national security and the safety of U.S. citizens. Despite the dangers of sharing this sensitive data with a company subject to Chinese control, Xandr knowingly shares sensitive information—including information like Plaintiff's and Subclass members' browsing activity, behavioral insights, and personal identifiers—with Temu.

90. The extent of Xandr's collection, enrichment, and redistribution of highly detailed identity profiles is staggering and highly offensive. These actions represent egregious breaches of social norms and violate both the reasonable expectation of privacy held by Plaintiff and the California Subclass members, and the constitutional right to privacy guaranteed under California law. Xandr lacks any legitimate business interest in covertly tracking, profiling, and aggregating the identities and private information of Plaintiff and the California Subclass members.

91. As a result of these extensive and intentional invasions of privacy, Plaintiff and California Subclass members have suffered harm and are entitled to just

compensation and injunctive relief.

THIRD CAUSE OF ACTION

Intrusion Upon Seclusion Under California Common Law (On behalf of Plaintiff and the California Subclass)

92. Plaintiff and the California Subclass members incorporate the foregoing allegations as if fully set forth herein.

93. Plaintiff and the California Subclass members have a strong interest in preventing the unauthorized collection, aggregation, and dissemination of their most personal information. These individuals maintain a reasonable expectation of privacy in their day-to-day lives—an expectation that extends not only to their Internet browsing activity and online communications, but also to the personal data that Xandr surreptitiously collects, enriches, de-anonymizes, and sells without the knowledge or consent of Plaintiff and the California Subclass members.

94. Xandr has violated Plaintiff's and the California Subclass members' reasonable expectation of privacy through its collection, aggregation, correlation, and dissemination of Plaintiff's and the California Subclass members' personal information. Xandr's practices are highly offensive to a reasonable person and constitute an egregious breach of social norms.

95. Xandr intentionally and extensively violates the reasonable expectation of privacy held by Plaintiff and the California Subclass members through engaging in covert, large-scale data collection designed to uniquely identify and surveil individuals. Xandr secretly harvests and correlates personal information, enriches that data with additional details, and builds highly detailed identity profiles unique to each individual. These profiles are then shared with potentially thousands of undisclosed third parties for profit through the RTB process.

96. Collecting detailed information about a person's device, behavior, or website usage while they engage with deeply personal content—such as a site

dedicated to the discussion of a chronic illness—is inherently intrusive. Most people would be shocked to learn that simply opening a webpage could trigger real-time data harvesting and the silent creation of a detailed behavioral profile tied to their identity. This covert surveillance and subsequent profiling would be highly offensive to a reasonable person and constitutes a profound violation of social norms.

97. Xandr does not merely collect isolated data points from Plaintiff and California Subclass members. It stockpiles a vast range of personal information, including persistent identifiers (e.g., cookie IDs, device IDs, mobile advertising IDs, and IP addresses), device metadata (e.g., screen resolution, browser version, operating system, and language settings), and contextual information such as full URLs and referring pages. This contextual data often reveals the exact content being viewed by the individual at the very moment Xandr broadcasts the data to bidders.

98. Through these practices, Xandr intercepts, tracks, collects, aggregates, and redistributes the Internet activity and communications of Plaintiff and Subclass members. Xandr's cookie-syncing processes further enable the linkage of user identifiers across websites, facilitating persistent cross-site tracking and user recognition, allowing Xandr to link activity across websites and sessions, building a detailed, persistent profile on each individual.

99. By combining its central role in the RTB ecosystem with technologies like JavaScript trackers, Prebid.js adapters, and cookie-syncing endpoints, Xandr compiles and constantly refines a previously unimaginable record of the attributes, Internet activity, and communications of Plaintiff and California Subclass members.

100. Xandr exploits this vast trove of data to create or assign segments to users—classifications that allow Xandr and its downstream partners to categorize each user in a highly granular manner. These detailed segments are not based only on demographic information but may also be based on deeply sensitive attributes like mental or physical health conditions, financial distress, disability, and religious

beliefs.

101. These segments are shared alongside uniquely identifying information, providing not just a detailed snapshot of the user's traits but the ability to permanently tie those traits to an infinitely expandable and re-shareable dossier on that individual. Xandr shares these profiles, including detailed segment data, with potentially thousands of unknown third parties. The information is distributed in real time and may also be retained by these downstream partners, creating additional copies of these dossiers that can be used, enhanced, and re-shared indefinitely. By facilitating this process, Xandr not only violates Plaintiff's and California Subclass members' reasonable expectation of privacy but also empowers downstream entities to do the same.

102. Correlating this data into rich behavioral profiles, then attaching persistent identifiers that allow advertisers to link the behavior to real-world identities is also highly offensive to a reasonable person. Moreover, sharing those profiles with countless undisclosed third parties for profit, without the user's knowledge or meaningful consent, is highly offensive behavior.

103. Among the third parties receiving this sensitive data is Temu, a foreign-owned company with its principal place of business in China. When Temu participates in an RTB auction through Xandr's exchange, it receives behavioral segment data, persistent identifiers, and the context of the web page being viewed. This allows Temu not only to serve targeted ads but also to retain and analyze that information for future use, thereby gaining deep visibility into users' habits, interests, and vulnerabilities.

104. As described above, the U.S. government has identified China and its control of personal data as adversarial to national security and the safety of U.S. citizens. Americans have a strong interest in protecting their personal data from an entity the U.S. government has identified as a threat to national security and the

safety of U.S. citizens. Despite the dangers of sharing this sensitive data with a company subject to Chinese control, Xandr knowingly shares sensitive information—including browsing activity, behavioral insights, and personal identifiers—with Temu.

105. The extent of Xandr's collection, enrichment, and redistribution of highly detailed identity profiles is staggering and highly offensive. These actions represent egregious breaches of social norms and violate the reasonable expectation of privacy held by Plaintiff and the California Subclass members. Xandr lacks any legitimate business interest in covertly tracking, profiling, and aggregating the identities and private information of Plaintiff and the California Subclass members.

106. As a result of these extensive and intentional invasions of privacy, Plaintiff and the California Subclass members have suffered harm and are entitled to just compensation and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Marissa Porcuna individually and on behalf of the Class and Subclass, pray for the following relief:

(a) An order certifying the Class and Subclass as defined above, appointing Plaintiff Marissa Porcuna as the representative of the Class and Subclass, and appointing their counsel as Class Counsel;

(b) A judgment holding that Defendant's actions, as set out above, violate the ECPA, 18 U.S.C. § 2510, *et seq*., with respect to Plaintiff and the Class, and that such actions violate the California Constitution and intrude upon the seclusion of Plaintiff and members of the California Subclass;

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

(d) A judgment awarding 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/ Brandt Silverkorn*
One of Plaintiff's Attorneys

Brandt Silverkorn (SBN 323530)
bsilverkorn@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the alleged Class and Subclass