BURSOR & FISHER, P.A.
Kaili C. Lynn (State Bar No. 334933)
Joshua R. Wilner (State Bar No. 353949)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: klynn@bursor.com
jwilner@bursor.com

BURSOR & FISHER, P.A.
Philip L. Fraietta (State Bar No. 354768)
50 Main Street, Suite 475
White Plains, NY 10606
Telephone: (914) 874-0710
Facsimile: (914) 206-3656
E-mail: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Max S. Roberts (State Bar No. 363482)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-mail: mroberts@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DANIEL YEE, individually and on behalf of all others similarly situated, Plaintiff, v. FANDANGO MEDIA, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **<u>JURY TRIAL DEMANDED</u>**

TABLE OF CONTENTS

PAGE(S)

NATURE OF THE ACTION 1

THE PARTIES 4

JURISDICTION AND VENUE 4

FACTUAL ALLEGATIONS 5

I. THE CALIFORNIA INVASION OF PRIVACY ACT 5

II. DEFENDANT VIOLATES THE CIPA 7

A. The Mechanics And Privacy Implications Of IP Addresses 8

1. Differentiating Between a Public Versus Private IP Address 8

2. Advertisers Use Public IP Addresses to Target Specific Households, and Data Brokers Attach IP Addresses to Comprehensive User Profiles To Identify An Individual 11

B. The Trackers On The Website Are "Pen Registers" 14

1. The ADNXS Tracker And The Data Brokers It Cookie-Syncs With on the Website 15

(i) PubMatic 19

(ii) The Rubicon/Magnite Tracker 20

2. The OpenX Tracker 22

3. The PubMatic Tracker And The Data Brokers It Cookie-Syncs With on the Website 25

(i) ID5 ID Tracker 27

(ii) Tapad/Experian Tracker 30

(iii) The Lijit/Sovrn Tracker 32

III. DEFENDANT'S CONDUCT CONSTITUTES AN INVASION OF PLAINTIFF'S AND CLASS MEMBERS' PRIVACY 36

A. Data Brokers and Real-Time Bidding: The Information Economy 37

1. Data Brokers 37

2. Real-Time Bidding 43

3. Cookie Syncing 48

B. Defendant Uses The ADNXS Tracker For Targeted Advertising And Data Monetization 52

C. Defendant Uses The Pubmatic Tracker For Identity Resolution, Targeted Advertising, And Data Monetization 53

D. Defendant Uses The OpenX Tracker For Identity Resolution, Targeted Advertising, And Data Monetization 56

IV. PLAINTIFF'S EXPERIENCE 59

CLASS ALLEGATIONS 62

CAUSES OF ACTION 63

PRAYER FOR RELIEF 66

JURY TRIAL DEMANDED 66

Plaintiff Daniel Yee ("Plaintiff") brings this action individually and on behalf of all others similarly situated against Fandango Media, LLC ("Fandango" or "Defendant"). Plaintiff makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. Defendant is a large digital network in the movie industry, owned by NBCUniversal and Warner Bros. Discovery, that serves over 45 million monthly users with ticketing purchases, reviews (Rotten Tomatoes), and streaming.[1] Defendant owns and operates several websites including its movie review site, RottenTomatoes.com, which receives approximately 37.88 million visits per month from the United States (the "Website").[2]

2. When users visit Defendant's Website, Defendant causes at least three Trackers—the ADNXS Tracker, the OpenX Tracker, and the PubMatic Tracker (collectively, the "Trackers")—to be installed on the internet browsers of the Website's visitors. The Trackers are operated by separate and distinct third parties: Microsoft Corporation ("Microsoft"), OpenX Technologies, Inc. ("OpenX"), and PubMatic Inc. ("PubMatic") respectively (together, the "Third Parties").

3. Through their respective Trackers, the Third Parties collect the Website's users' internet protocol ("IP") addresses and other device identifier information such as device type, browser type, and unique and persistent identifiers ("Device Metadata"). The Third Parties' Trackers also set a cookie that includes a unique user identifier, which the Trackers collect on subsequent visits, and which is used by the Third Parties to identify and deanonymize the user.

4. Defendant and the Third Parties use the data collected by the Trackers to identify and de-anonymize users, hyper-target advertisements to users, and to enrich themselves.

[1] FANDANGO, https://www.fandango.com/about-us#:~:text=Fandango%20Media%20is%20the%20ultimate,Career%20Opportunities

[2] SEMRUSH, https://www.semrush.com/website/rottentomatoes.com/overview/.

5. Because the Trackers capture the Website's visitors' "routing, addressing, or signaling information," the Trackers each constitute a "pen register" under Section 638.50(b) of the California Invasion of Privacy Act ("CIPA"). (Cal. Penal Code § 638.50(b).)

6. By installing and using the Trackers without Plaintiff's prior consent and without a court order, Defendant violated CIPA § 638.51(a).

7. The allegations here are made more invasive by the entities operating the Trackers and collecting Plaintiff's and Class Members' IP Addresses and Device Metadata. OpenX[3] and PubMatic[4] are registered data brokers in California that focus on identifying and de-anonymizing users through identity resolution services. The purpose of this is to enrich the value of Defendant's Website users by linking those users' IP addresses and Device Metadata to profiles that contain as much personal and demographic information as possible. This prevents users from being anonymous when they visit the Website. Users are then offered up for sale with all this collated information to interested advertisers in the "real-time bidding economy," with advertisers placing bids through platforms like Microsoft's. Advertisers can then target users of the Website better based on these attributes and will therefore pay Defendant more to show advertisements to Defendant's users. And the Third Parties share all this data between each other and with various other entities through a process called "cookie syncing," meaning Plaintiff's and Class Member's information winds up in the hands of untold numbers of third parties, without consent.

8. In sum, Defendant's scheme is to tie users' browsing activity on the Website with personal information disclosed on other sites—all captured by the Trackers—to sell this collated information to advertisers. All of this enriches Defendant through advertising revenue, makes the Third Parties' services (*i.e.*, their Trackers) more valuable to Defendant and other customers, and strips Plaintiff and Class Members of their anonymity and privacy in the process.

[3] *Data Broker Registration for OpenX Technologies, Inc.*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-broker/registration/193614.

[4] *Data Broker Registration for PubMatic, Inc.*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-broker/registration/186702.

9. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents, and to recover statutory damages for Defendant's violation of CIPA § 638.51.

10. This is not the first time Defendant has faced class action lawsuits[5] and regulatory action over its privacy violations. Notably, the Federal Trade Commission ("FTC") sued Fandango on August 19, 2014 for its failure to ensure the secure transmission of "consumers' sensitive personal information, including credit card information and social security numbers" on its mobile apps, making the sensitive information "vulnerable to interception by third parties."[6]

11. Specifically, the FTC's complaint alleged that Defendant "disabled a process called SSL certificate verification that would have protected consumers' information."[7] Fandango reached a settlement for its violations of provisions of the Federal Trade Commission Act, agreeing to "establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent's products or services."[8]

12. Defendant also agreed to "not misrepresent in any manner, expressly or by implication, the extent to which respondent or its products or services maintain and protect the privacy, security, confidentiality, or integrity of any covered information."[9] According to the Settlement Order, "covered information" is defined as "information from or about an individual consumer, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact

[5] CLASSACTION.ORG, https://www.classaction.org/news/category/fandango-media-llc.

[6] *FTC Approves Final Orders Settling Charges Against Fandango and Credit Karma,* FEDERAL TRADE COMMISSION (Aug. 19, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/08/ftc-approves-final-orders-settling-charges-against-fandango-credit-karma.

[7] *Id*.

[8] Settlement Order, *In the Matter of Fandango, LLC*, No. C 4481, (Aug. 13, 2014), https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf at 3.

[9] *Id*. at 2.

information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license or other state issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; (j) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; or (k) an authentication credential, such as a username or password."[10]

13. Now Defendant is ignoring and violating the requirements of CIPA because it installed Trackers (pen registers) on its Website and did not obtain prior consent from Plaintiff and Class Members before allowing the Third Parties to use their respective Trackers to intercept Website users' communications with Defendant.

THE PARTIES

14. Plaintiff Daniel Yee is a California citizen who, at all relevant times, resided in San Ramon, California. At all relevant times, Plaintiff Yee was in California when he visited Defendant's Website rottentomatoes.com.

15. Defendant Fandango Media, LLC is a Virginia limited liability company which maintains its headquarters in Universal City, California,[11] with additional offices and operations in Los Angeles.[12]

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(a) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00 exclusive of interest and costs, there are over 100 members of the putative class, and at least one class member is a citizen of a different state than Defendant.

[10] *Id.*

[11] ZOOMINFO, https://www.zoominfo.com/pic/fandango-media-llc/13910366; *see also* CRAFT, https://craft.co/fandango/locations#:~:text=Fandango%20is%20headquartered%20in%20Beverly%20Hills%2C%20407,United%20States%2C%20and%20has%201%20office%20location.

[12] FANDANGO, https://www.fandango.com/about-us.

17. This Court has jurisdiction over Defendant because Defendant is headquartered in California.

18. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial portion of the events giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

I. THE CALIFORNIA INVASION OF PRIVACY ACT

19. The California Legislature enacted CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

20. As the California Supreme Court has held in explaining the purpose behind the CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—*the right to control the nature and extent of the firsthand dissemination of his statements*.

Ribas v. Clark 38 Cal. 3d 355, 360-61 (1985) (emphasis added; internal citations omitted).

21. As relevant here, CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

22. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

23. A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing,

or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(b).

24. In plain English, a "pen register" is a "device or process" that records *outgoing* information, while a "trap and trace device" is a "device or process" that records *incoming* information.

25. Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology advanced, however, courts have expanded the application of these surveillance devices to Internet tracking technology.

26. For example, if a user sends an email, a "pen register" might record the email address it was sent from because this is the user's *outgoing* information. On the other hand, if that same user receives an email, a "trap and trace device" might record the email address it was sent from because this is *incoming* information that is being sent to that same user.

27. Although CIPA was enacted before the dawn of the Internet, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013); *see also*, *e.g.*, *Shah v. Fandom, Inc*, 754 F. Supp. 3d 924, 930 (N.D. Cal. 2024) (finding trackers similar to those at issue here were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC,* 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Lesh v. Cable News Network, Inc.*, 767 F.Supp.3d 33 (S.D.N.Y. Feb. 20, 2025) (same); *Moody v. C2 Educ. Sys. Inc.* 742 F. Supp. 3d 1072, 1077 (C.D. Cal. 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and 638.51."); *Greenley v. Kochava, Inc.* 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v. Assurance IQ, LLC* 2022 WL 1744107 (9th Cir. May 31, 2022), at *1 ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications.").

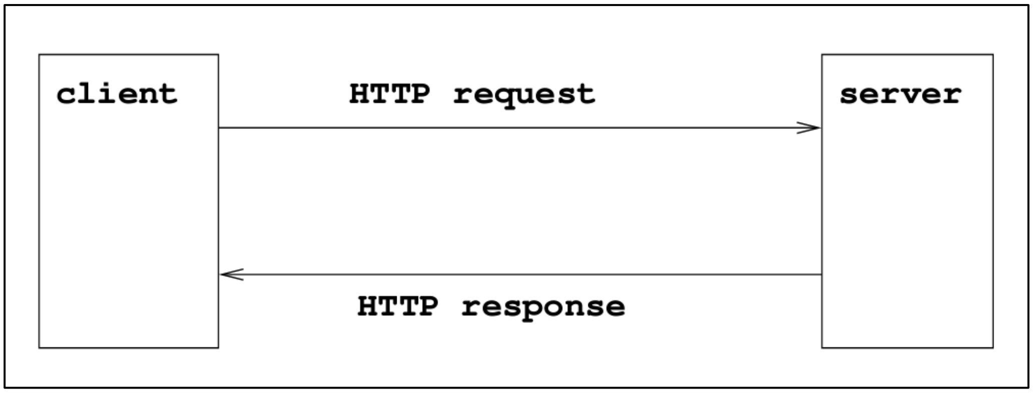
28. This accords with the fact that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.* 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

29. Individuals may bring an action against the violator of any provision of CIPA—including CIPA § 638.51—for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

II. DEFENDANT VIOLATES THE CIPA

30. To make Defendant's Website load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to Defendant's server where the relevant Website's data is stored. In response to the request, Defendant's server sends an "HTTP response" back to the browser with a set of instructions. A general diagram of this process is pictured at Figure 1, which explains how Defendant's Website transmits instructions back to users' browsers in response to HTTP requests.

Figure 1:



31. The server's instructions include how to properly display the Website —*e.g.*, what images to load, what text should appear, or what music should play.

32. In addition, the server's instructions cause the Trackers to be installed on a user's browser. The Trackers then cause the browser to send identifying information—including the user's IP address and Device Metadata—to the Third Parties.

33. The Third Parties' Trackers will also set a cookie corresponding with a user ID unique to their Tracker that also allows the user to be tracked across the Internet and have their information synced between multiple entities.

34. Because, as described below, the Trackers collect users' addressing, routing, or signaling information—IP addresses, Device Metadata, and/or the unique user IDs—the Trackers are pen registers.

35. Plaintiff and Class Members did not provide their prior consent to Defendant to install the Trackers on their browsers or use the Trackers. Nor did Defendant obtain a court order before installing or using the Trackers.

A. The Mechanics And Privacy Implications Of IP Addresses

36. An IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). The traditional format of IP addresses is called IPv4, and it has a finite amount of combinations and thus is limited to approximately 4.3 billion addresses. Because this proved to be insufficient as the Internet grew, IPv6 was introduced. IPv6 offers a vastly larger address space with 340 undecillion possible addresses. While IPv6 adoption has been increasing, many networks still rely on IPv4.[13]

37. Much like a telephone number, an IP address guides or routes an intentional communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential for identifying a device on the internet or within a local network, facilitating smooth communication between devices.

1. Differentiating Between a Public Versus Private IP Address

38. A public IP address is accessible from anywhere on the internet; it is assigned by an Internet Service Provider ("ISP") and it is unique globally. Public IP addresses are required for devices that need direct internet access.

[13] *See, e.g.*, *What is the Internet Protocol*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/internet-protocol/; Stefano Gridelli, *What is an RFC1918 Address?*, NETBEEZ (Jan. 22, 2020), https://netbeez.net/blog/rfc1918/.

39. While public IP addresses are unique, they are not necessarily “public” in the sense that they are freely accessible. If an individual is not actively sending data packets out, the public IP address remains private and is not broadcast to the wider internet.

40. Public IP addresses can be used to determine the approximate physical location of a device. For example, services like iplocation.io use databases that map IP addresses to geographic areas—often providing information about the country, city, approximate latitude and longitude coordinates, or even the internet service provider associated with the public IP. This geolocation capability is leveraged by online advertising and user identification services.

41. A private IP address is used within an internal network and is not routable on the public internet. The Internet Assigned Numbers Authority (“IANA”) reserves specific ranges of numbers to be exclusively used for private IP addresses (*e.g.*, 172.16.0.0 through 172.31.255.255). Thus, private IP addresses can be used repeatedly across different networks because they are isolated from the global internet. For example, a home network in New York and an office network in Tokyo can both use the same private IP address (*e.g.*, 192.168.1.1) for their routers without conflict.

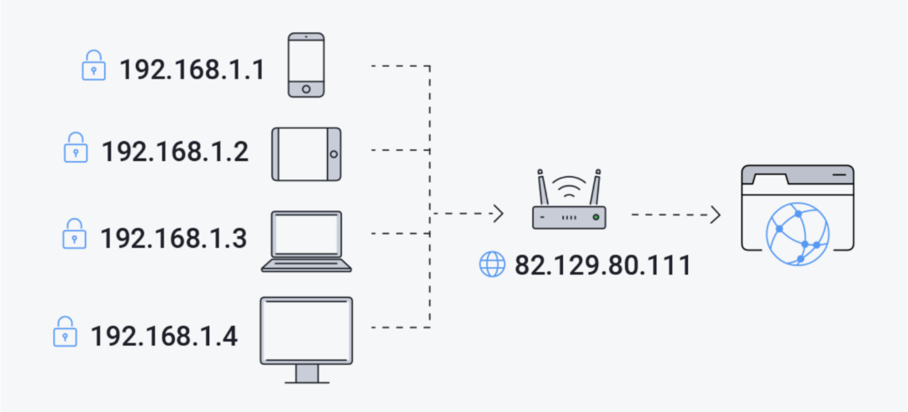
42. The distinction between a public and private IP address is fundamental to the architecture of modern networks. Public IP addresses facilitate global communication, while private IP addresses conserve the finite amount of combinations to make an IP address through local network communication. And crucially, a private IP address does not divulge a user’s geolocation, whereas a public IP address does and is thus extensively used in advertising.

43. An analogy is useful. A public IP address is like the number for a landline telephone for a household. A private IP address is like each handset that is connected to that landline number (*e.g.*, “Handset #1,” “Handset #2”). The public IP address determines the phone number who is making the call, which provides the most identifying information. On the other hand, knowing whether Handset #1 versus Handset #2 is making a call allows one to distinguish between members of the same household, although less can be gleaned from this fact on its own.

44. The same is true of IP addresses. The public IP address divulges the approximate location of the user that is connecting to the Internet and the router directing those communications (presumably the user’s house or workplace), and it is the means through which the user

communicates with the website and the Internet at large. The private IP address then distinguishes between the devices in the same household accessing the Internet from this location point.[14]

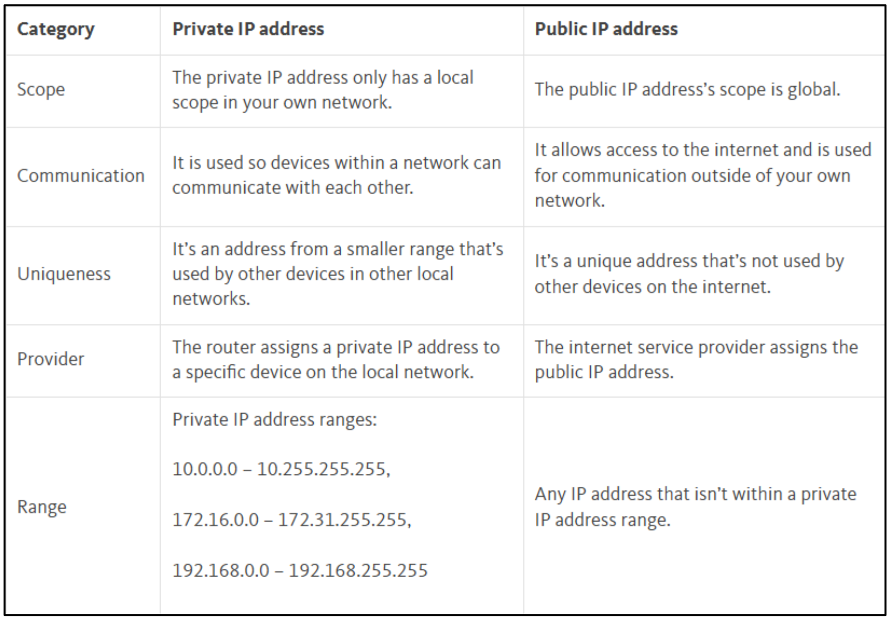
Figure 2:



Each device on a network has a private IP address, and the router has a public IP address to communicate with the rest of the internet.

45. Thus, the differences between public and private IP addresses are as follows:[15]

Figure 3:



Category	Private IP address	Public IP address
Scope	The private IP address only has a local scope in your own network.	The public IP address's scope is global.
Communication	It is used so devices within a network can communicate with each other.	It allows access to the internet and is used for communication outside of your own network.
Uniqueness	It's an address from a smaller range that's used by other devices in other local networks.	It's a unique address that's not used by other devices on the internet.
Provider	The router assigns a private IP address to a specific device on the local network.	The internet service provider assigns the public IP address.
Range	Private IP address ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255	Any IP address that isn't within a private IP address range.

[14] While the Trackers do not collect private IP addresses, as discussed below, the Trackers collect Device Metadata that distinguishes between devices accessing the same public IP address in the same way a private IP address would. By installing the Trackers on Website users' browsers, Defendant allows third parties to collect information that is analogous to a telephone number (the public IP address) and the specific handset that is making the call (the Device Metadata).

[15] *What's The Difference Between A Public And Private IP Address?*, AVIRA (Jan. 31, 2024), https://www.avira.com/en/blog/public-vs-private-ip-address.

46. A public IP address is therefore "routing, addressing, or signaling information."

47. A public IP address is "addressing" information because it determines the general geographic coordinates of the user who is accessing a website.

48. A public IP address is "routing" or "signaling" information because it is sending or directing the user's communication from the router in their home or work to the website they are communicating with, and ensuring that "emails, websites, streaming content, and other data reaches you correctly."[16]

2. *Advertisers Use Public IP Addresses to Target Specific Households, and Data Brokers Attach IP Addresses to Comprehensive User Profiles To Identify An Individual*

49. Through a public IP address, a device's state, city, zip code, and approximate latitude and longitude can be determined. Thus, knowing a user's public IP address—and therefore geographical location—"provide[s] a level of specificity previously unfound in marketing."[17]

50. A public IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[18] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests."[19] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[20] because "[c]ompanies can use an IP address … to personally identify individuals."[21]

51. In fact, a public IP address is a common identifier used for "geomarketing," which is "the practice of using location data to identify and serve marketing messages to a highly targeted audience. Essentially, geomarketing allows [websites] to better serve [their] audience by giving

[16] Anthony Freda, *Private IP vs Public IP: What's the Difference?*, AVG (June 4, 2021), https://www.avg.com/en/signal/public-vs-private-ip-address.

[17] *IP Targeting: Understanding This Essential Marketing Tool*, AccuData (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[18] *Location-Based Targeting That Puts You in Control*, Choozle, https://choozle.com/geotargeting-strategies/.

[19] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov. 29, 2023), https://tinyurl.com/54j8hj5b.

[20] *IP Targeting: Understanding This Essential Marketing Tool*, AccuData (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[21] Trey Titone, *The Future Of Ip Address As An Advertising Identifier*, Ad Tech Explained (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.

[them] an inside look into where they are, where they have been, and what kinds of products or services will appeal to their needs."[22] For example, for a job fair in a specific city, companies can send advertisements to only those in the general location of the upcoming event.[23]

52. "IP targeting is a highly effective digital advertising technique that allows you to deliver ads to specific physical addresses based on their internet protocol (IP) address. IP targeting technology works by matching physical addresses to IP addresses, allowing advertisers to serve ads to specific households or businesses based on their location."[24]

53. "IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This means that advertisers can deliver highly targeted ads to specific households or businesses, rather than relying on more general demographics or behavioral data."[25]

54. Thus, when Defendant installs and uses the Third Parties' Trackers, it knows its conduct is specifically targeting and affecting Californians based on the public IP addresses.

55. In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's public IP address because it "can be more cost-effective than other forms of advertising."[26] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[27]

56. Moreover, "IP address targeting can help businesses to improve their overall marketing strategy."[28] "By analyzing data on which households or businesses are responding to their

[22] *See, e.g.*, *The Essential Guide to Geomarketing: Strategies, Tips & More*, Deep Sync (Nov. 20, 2023), https://deepsync.com/geomarketing/.

[23] *See, e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GeoFli, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns.

[24] *IP Targeting*, Savant DSP, https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB.

[25] *Id.*

[26] Herbert Williams, *The Benefits of IP Address Targeting for Local Busines*ses, LinkedIn (Nov. 29, 2023), https://tinyurl.com/54j8hj5b.

[27] *Id.*

[28] *Id.*

ads, businesses can refine their targeting strategy and improve their overall marketing efforts."[29]

57. The collection of IP addresses here is particularly invasive given several of the Third Parties' statuses as data brokers. As a report from NATO found:

> [a] data broker may receive information about a[] [website] user, including his … IP address. The user then opens the [website] while his phone is connected to his home Wi-Fi network. When this happens, the data broker can use the IP address of the home network to identify the user's home, and append this to the unique profile it is compiling about the user. If the user has a computer connected to the same network, this computer will have the same IP address. The data broker can then use the IP address to connect the computer to the same user, and identify that user when their IP address makes requests on other publisher pages within their ad network. Now the data broker knows that the same individual is using both the phone and the computer, which allows it to track behaviour across devices and target the user and their devices with ads on different networks.[30]

58. In other words, not only does the collection of IP addresses by the Third Parties cause harm in and of itself, but OpenX and PubMatic, as registered data brokers, also specifically attach IP addresses to their comprehensive user profiles, tracking Plaintiff and Class Members across the Internet using their IP addresses and compiling vast reams of other personal information in the process.

59. For these reasons, under Europe's General Data Protection Regulation, IP addresses are considered "personal data, as they can potentially be used to identify an individual."[31]

60. Likewise, under the California Consumer Privacy Act ("CCPA"), a law separate from CIPA but related to it, IP addresses are considered "personal information" because they are

[29] *Id.*

[30] HENRIK TWETMAN & GUNDARS BERGMANIS-KORATS, NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, DATA BROKERS AND SECURITY at 11 (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[31] *Is an IP Address Personal Data?, Convesio*, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/; *see also What Is Personal Data?*, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.

"reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1)(A).[32]

61. As alleged below, Defendant installs the Trackers on Website users' browsers for marketing and analytics purposes, and the Trackers collect information—users' IP addresses—that identifies the outgoing "routing, addressing, or signaling information" of the user. Accordingly, the Trackers are each "pen registers."

62. Thus, any time a user visits the Website, Defendant will cause the Trackers to be installed on users' browsers, and those Trackers will collect the user's IP address and Device Metadata.

B. The Trackers On The Website Are "Pen Registers"

63. Defendant owns and operates the Webiste.

64. When some companies build their websites, they install or integrate various third-party scripts into the code of the website to collect data from users or perform other functions.[33]

65. Often, third-party scripts are installed on websites "for advertising purposes."[34]

66. Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time."[35]

67. Defendant has incorporated the Trackers' code into the code of its Website, including when Plaintiff Yee and Class Members visited the Website.

68. When Plaintiff Yee and Class Members visited the Website, the Website's code—as programmed and installed by Defendant—caused the Trackers to be installed on Plaintiff's and Class

[32] A "consumer" is defined as "a natural person who is a California resident." Cal. Civ. Code § 1798.140(i).) A "household" is defined as "a group … of consumers who cohabitate with one another at the same residential address and share use of common devices or services." Cal. Civ. Code § 1798.140(1).)

[33] *See Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ ("Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user's visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user's browsing history to other companies…").

[34] *Id.*

[35] *Id.*

Members' browsers. This allowed the Third Parties—through their respective Trackers—to collect Plaintiff's and Class Members' IP addresses and Device Metadata and pervasively track them across the Internet.

69. The Trackers also cause additional data points to be sent from Plaintiff's and Class Members' browser to the Third Parties, which are meant to uniquely identify users across sessions and devices. In addition to the public IP address, key elements include the user-agent string (browser, operating system, and device type) and device capabilities such as supported image formats and compression methods. Persistent identifiers like the PUID, GUID, UID, PSVID, and User-Agent ensure users can be tracked even after clearing standard session data like cookies. Advanced methods like fingerprinting and server-side matching remain unaffected by cookie deletion. Combined, these elements form a detailed, unique fingerprint that allows for cross-site tracking and behavioral profiling.

70. Defendant and the Third Parties then use the public IP addresses, Device Metadata, and unique identifiers of Website visitors that are collected and set by the Trackers, including those of Plaintiff Yee and Class Members, to deanonymize Plaintiff and Class Members, serve hyper-targeted advertisements, and unjustly enrich themselves through this improperly collected information.

71. At no time prior to the installation and use of the Trackers on Plaintiff's and Class Members's browsers, or prior to the use of the Trackers, did Defendant procure Plaintiff's and Class Members' consent for such conduct. Nor did Defendant obtain a court order to install or use the Trackers.

1. The ADNXS Tracker And The Data Brokers It Cookie-Syncs With on the Website

72. Microsoft Corporation is a technology company with software-as-a-service products, such as Microsoft Advertising. Microsoft owns and operates the ADNXS Tracker, which it provides to website owners like Defendant for a fee. Microsoft rebranded ADNXS to "Microsoft Invest," but the two are the same service.

73. In 2022, when Microsoft formally acquired AT&T's ad-tech business, Xandr, it provided Microsoft with demand- and sell-side platforms which Xandr operated.[36] Thus, the ADNXS Tracker functions as both a demand-side platform or "DSP" and a sell-side platform or "SSP" and both terms are explained in more detail below. According to Microsoft, the ADNXS Tracker is "a strategic buying platform built for the needs of today's advertisers looking to invest in upper funnel buying and drive business results."[37] Its "platform is a real-time bidding system and ad server."[38]

74. In other words, Microsoft facilitates the selling of Defendant's Website users to interested advertisers, who will bid to show those users advertisements targeted to their identity and location through its ADNXS Tracker. This process enables Defendant to monetize its Website. To achieve this, Microsoft uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

75. When a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the ADNXS Tracker on the user's browser. The ADNXS Tracker, in turn, instructs the user's browser to send Microsoft the user's IP address and Device Metadata—which Microsoft records and decodes—as the below screenshot from Plaintiff Yee's browser on the Website indicates (relevant portions highlighted in blue and red boxes).[39]

//

//

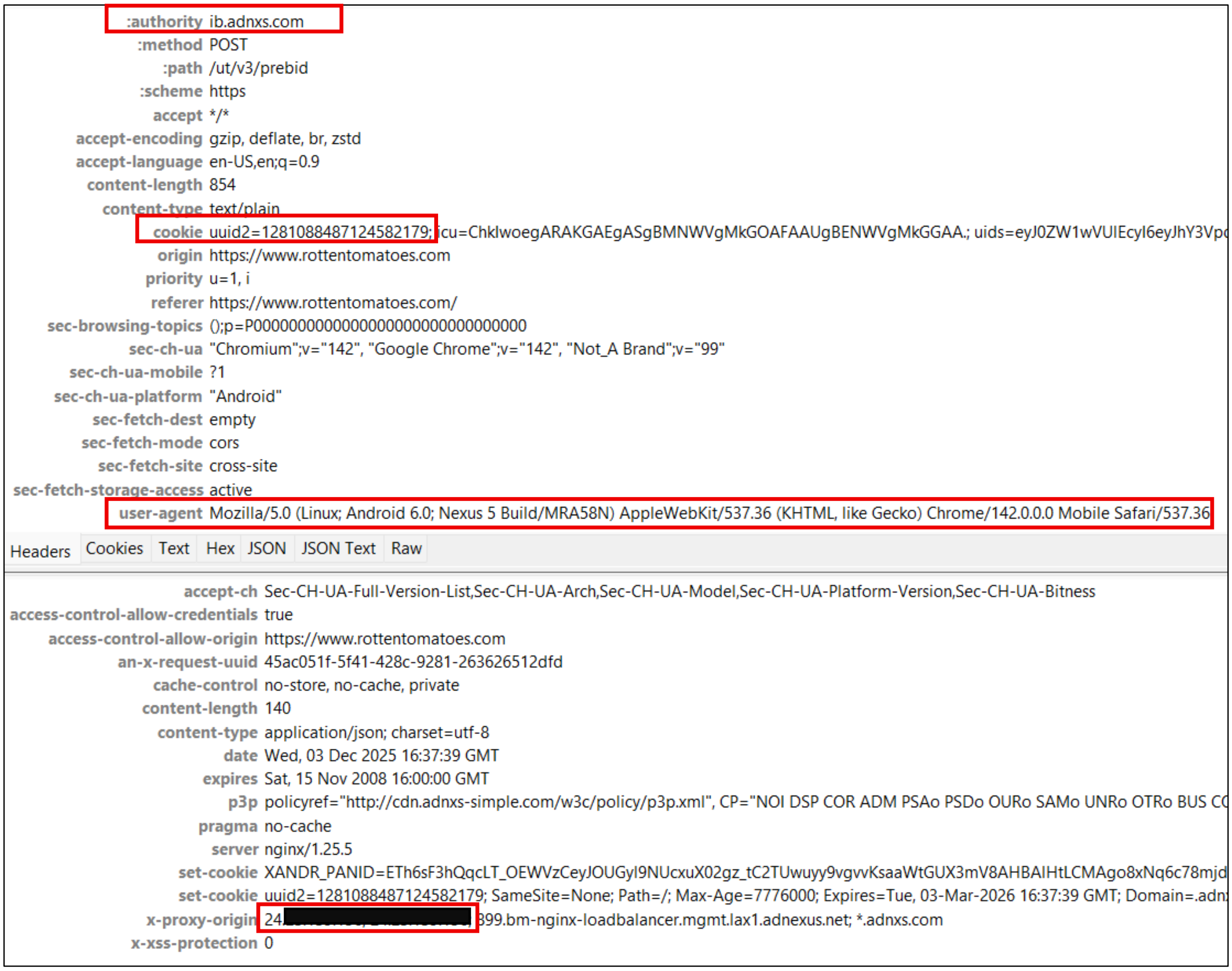
[36] *AT&T Sells Xandr to Microsoft: Microsoft and Xandr have been working together for more than 10 years*, ADWEEK, (Dec. 21, 2021), https://www.adweek.com/programmatic/att-sells-xandr-to microsoft/#:~:text=Microsoft%20and%20Xandr%20have%20been%20working%20together%20for%20more%20than%2010%20years&text=AT&T%20launched%20Xandr%2C%20named%20for%20Alexander%20Graham%20Bell%2C%20in%202018.&text=Microsoft%20will%20acquire%20AT&T's%20ad,Financial%20details%20weren't%20released.

[37] *About Microsoft Invest*, MICROSOFT IGNITE (Feb. 12, 2024), https://learn.microsoft.com/en-us/xandr/invest/about-invest.

[38] *Id.*

[39] All but the first two numbers of Plaintiff's IP address are redacted throughout this Complaint to protect his privacy. The screenshot shows his IP address disclosed next to the "x-proxy origin" label at the bottom of the image.

Figure 4:



```
             :authority ib.adnxs.com
                :method POST
                  :path /ut/v3/prebid
                :scheme https
                 accept */*
        accept-encoding gzip, deflate, br, zstd
        accept-language en-US,en;q=0.9
         content-length 854
           content-type text/plain
                 cookie uuid2=1281088487124582179; icu=ChkIwoegARAKGAEgASgBMNWVgMkGOAFAAUgBENWVgMkGGAA.; uids=eyJ0ZW1wVUlEcyI6eyJhY3Vp
                 origin https://www.rottentomatoes.com
               priority u=1, i
                referer https://www.rottentomatoes.com/
    sec-browsing-topics ();p=P0000000000000000000000000000000
              sec-ch-ua "Chromium";v="142", "Google Chrome";v="142", "Not_A Brand";v="99"
       sec-ch-ua-mobile ?1
     sec-ch-ua-platform "Android"
         sec-fetch-dest empty
         sec-fetch-mode cors
         sec-fetch-site cross-site
sec-fetch-storage-access active
             user-agent Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Mobile Safari/537.36
```

```
                       accept-ch Sec-CH-UA-Full-Version-List,Sec-CH-UA-Arch,Sec-CH-UA-Model,Sec-CH-UA-Platform-Version,Sec-CH-UA-Bitness
access-control-allow-credentials true
     access-control-allow-origin https://www.rottentomatoes.com
               an-x-request-uuid 45ac051f-5f41-428c-9281-263626512dfd
                   cache-control no-store, no-cache, private
                  content-length 140
                    content-type application/json; charset=utf-8
                            date Wed, 03 Dec 2025 16:37:39 GMT
                         expires Sat, 15 Nov 2008 16:00:00 GMT
                             p3p policyref="http://cdn.adnxs-simple.com/w3c/policy/p3p.xml", CP="NOI DSP COR ADM PSAo PSDo OURo SAMo UNRo OTRo BUS C
                          pragma no-cache
                          server nginx/1.25.5
                      set-cookie XANDR_PANID=ETh6sF3hQqcLT_OEWVzCeyJOUGyl9NUcxuX02gz_tC2TUwuyy9vgvvKsaaWtGUX3mV8AHBAIHtLCMAgo8xNq6c78mjd
                      set-cookie uuid2=1281088487124582179; SameSite=None; Path=/; Max-Age=7776000; Expires=Tue, 03-Mar-2026 16:37:39 GMT; Domain=.adn
                  x-proxy-origin 24[redacted]399.bm-nginx-loadbalancer.mgmt.lax1.adnexus.net; *.adnxs.com
                x-xss-protection 0
```

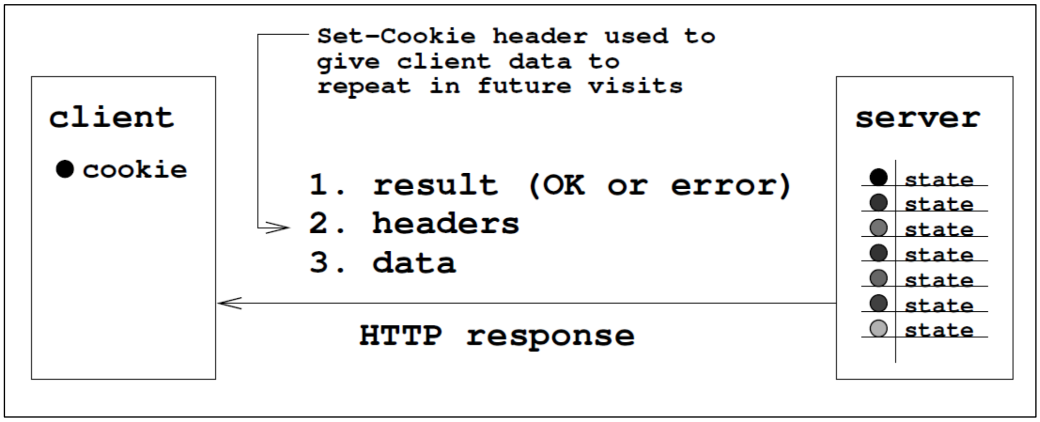
76. Moreover, Microsoft stores a cookie (the unique identifier, "UUID2" after "set cookie" in Figure 4 above) with the user's IP address and Device Metadata in the user's browser cache. The UUID2 "records information that helps differentiate between devices and browsers. This information is used to pick out ads delivered by the platform and assess the ad performance and its attribute payment."[40]

77. When the user subsequently visits Defendant's Website, the ADNXS Tracker locates the cookie identifier stored on the user's browser. If UUID2 is stored on the browser, the ADNXS Tracker causes the browser to send the UUID2 along with the user's IP address and Device Metadata to Microsoft.

[40] ATFX, COOKIE POLICY, https://www.atfxconnect.com/en/cookies-policy/.

78. Using the UUID2, IP addresses, and Device Metadata, Microsoft can track and identify Website users across the Internet. A general diagram of this process is pictured in Figure 5 below, which explains how the Website causes the ADNXS Tracker to install a cookie on the user's browser and instructs the user's browser to send the user's IP address and Device Metadata along with the UUID2.

Figure 5:



79. Microsoft also stores a cookie with the user's IP address in the user's browser cache. When the user subsequently visits Defendant's Website, the ADNXS Tracker locates the cookie identifier stored on the user's browser. If the cookie is stored on the browser, the ADNXS Tracker causes the browser to send the cookie along with the user's IP address to Microsoft. (*See* Figure 1, *supra*).

80. If the user clears his or her cookies, then the user wipes out the ADNXS Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the ADNXS Tracker on the user's browser, (ii) the ADNXS Tracker instructs the browser to send Microsoft the user's IP address and Device Metadata, (iii) the ADNXS Tracker stores a cookie in the browser cache, and (iv) Microsoft will continue to receive the user's IP address and Device Metadata on subsequent visits to the Website as part of the cookie transmission.

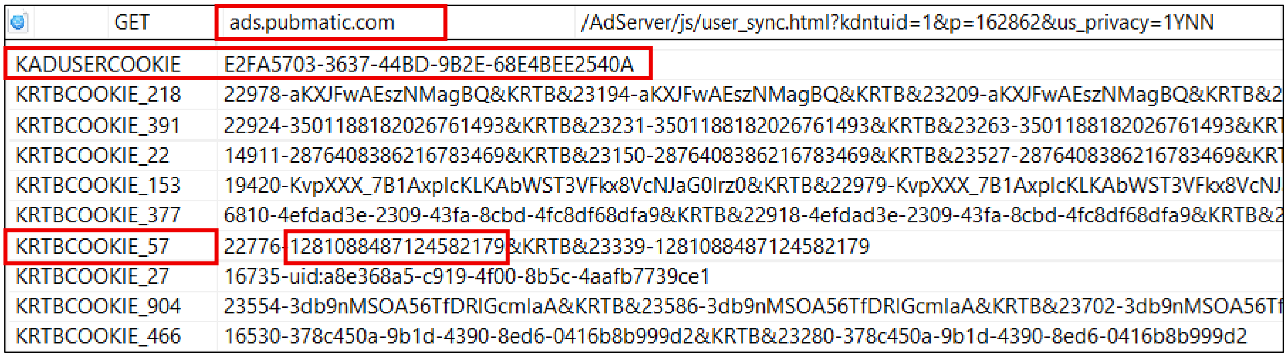
81. In all cases, however, Microsoft receives a user's IP address, Device Metadata, and unique UUID2 identifier every time its Tracker is loaded by the Website, as the above screenshot indicates.

82. Microsoft is also syncing its unique user identifier with PubMatic[41] and Magnite[42], both of which are registered data brokers in California.

(i) **PubMatic**

83. Microsoft syncs its UUID2 with the PubMatic Tracker, as Figure 6 shows. As pictured in the below screenshot from Plaintiff Yee's browser on the Website (relevant portions in red boxes), the value of the "KRTBCOOKIE_57" parameter matches the value of the UUID2 parameter in Figure 4 above. This allows Microsoft to obtain whatever information PubMatic has on the user (and vice versa). Indeed, PubMatic admits that the KRTBCOOKIEs are used "to correlate our user IDs with those of our partners (such as demand side platform clients or other advertising technology companies). We pass the information stored by the partner in this cookie to the partner when it is considering whether to purchase advertisements. This enables the partner to make better decisions about whether to display an advertisement to you."[43] PubMatic also sets a KADUSERCOOKIE on the user's browser (which is likewise syncing with the ADNXS Tracker), which is used to "uniquely identify each browser or device from which an individual user visits our partners' websites."[44]

Figure 6:



GET ads.pubmatic.com /AdServer/js/user_sync.html?kdntuid=1&p=162862&us_privacy=1YNN

KADUSERCOOKIE	E2FA5703-3637-44BD-9B2E-68E4BEE2540A
KRTBCOOKIE_218	22978-aKXJFwAEszNMagBQ&KRTB&23194-aKXJFwAEszNMagBQ&KRTB&23209-aKXJFwAEszNMagBQ&KRTB&2
KRTBCOOKIE_391	22924-3501188182026761493&KRTB&23231-3501188182026761493&KRTB&23263-3501188182026761493&KRT
KRTBCOOKIE_22	14911-2876408386216783469&KRTB&23150-2876408386216783469&KRTB&23527-2876408386216783469&KRT
KRTBCOOKIE_153	19420-KvpXXX_7B1AxplcKLKAbWST3VFkx8VcNJaG0lrz0&KRTB&22979-KvpXXX_7B1AxplcKLKAbWST3VFkx8VcNJ
KRTBCOOKIE_377	6810-4efdad3e-2309-43fa-8cbd-4fc8df68dfa9&KRTB&22918-4efdad3e-2309-43fa-8cbd-4fc8df68dfa9&KRTB&2
KRTBCOOKIE_57	22776-1281088487124582179&KRTB&23339-1281088487124582179
KRTBCOOKIE_27	16735-uid:a8e368a5-c919-4f00-8b5c-4aafb7739ce1
KRTBCOOKIE_904	23554-3db9nMSOA56TfDRIGcmlaA&KRTB&23586-3db9nMSOA56TfDRIGcmlaA&KRTB&23702-3db9nMSOA56Tf
KRTBCOOKIE_466	16530-378c450a-9b1d-4390-8ed6-0416b8b999d2&KRTB&23280-378c450a-9b1d-4390-8ed6-0416b8b999d2

84. PubMatic is another of the Third Parties, and so the capabilities of its Tracker are

[41] *Data Broker Registration for PubMatic, Inc.*, OFFICE OF THE ATTORNEY GENERAL DATA BROKER, https://oag.ca.gov/data-broker/registration/186702.

[42] *Data Broker Registration for Magnite, Inc.*, OFFICE OF THE ATTORNEY GENERAL DATA BROKER, https://oag.ca.gov/data-broker/registration/568127.

[43] PLATFORM COOKIE & OTHER SIMILAR TECHNOLOGIES POLICY, PUBMATIC, https://pubmatic.com/legal/platform-cookie-policy/.

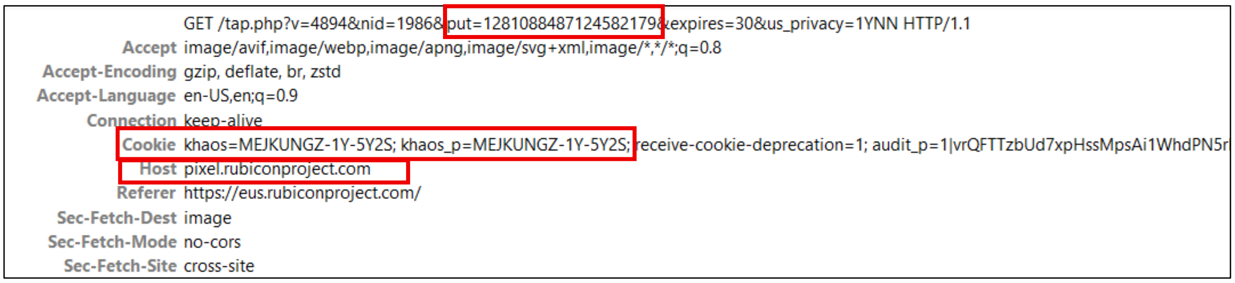
[44] *Id.*

described in more detail below. The long and short though, is that PubMatic enables website owners like Defendant to effectively sell their user's information to advertisers in a de-anonymized, targeted format by syncing its Tracker with the ADNXS Tracker. This enables Defendant's users to be de-anonymized and identified by being matched to comprehensive profiles and targeted with advertisements based on those profiles, thus driving advertising revenue for Defendant.

(ii) <u>The Rubicon/Magnite Tracker</u>

85. As another example, the ADNXS Tracker also syncs with the Rubicon Tracker owned by Magnite, which Defendant also installs and uses on Website users' browsers. As the below screenshot from Plaintiff's browser indicates, the value of the "put=" parameter below matches the value of the "UUID2" in Figure 4. Magnite is also enhancing the information Microsoft knows about Plaintiff with information that Magnite knows about Plaintiff. Finally, Magnite is installing its own cookie (the unique identifier, "khaos" in the screenshot below) on Plaintiff's browser for further tracking, syncing, and de-anonymization.

<u>Figure 7:</u>



```
                 GET /tap.php?v=4894&nid=1986&put=1281088487124582179&expires=30&us_privacy=1YNN HTTP/1.1
           Accept image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
  Accept-Encoding gzip, deflate, br, zstd
  Accept-Language en-US,en;q=0.9
       Connection keep-alive
           Cookie khaos=MEJKUNGZ-1Y-5Y2S; khaos_p=MEJKUNGZ-1Y-5Y2S; receive-cookie-deprecation=1; audit_p=1|vrQFTTzbUd7xpHssMpsAi1WhdPN5r
             Host pixel.rubiconproject.com
          Referer https://eus.rubiconproject.com/
   Sec-Fetch-Dest image
   Sec-Fetch-Mode no-cors
   Sec-Fetch-Site cross-site
```

86. Magnite is a registered data broker in California.[45] Magnite is a supply-side platform that companies like Defendant use "to monetize their content," and "[t]he world's leading agencies and brands trust [Magnite's] platform to access … billions of advertising transactions each month."[46]

[45] *Data Broker Registration for Magnite, Inc.*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-broker/registration/568127.

[46] *iHeartMedia and Magnite Unify Access to Broadcast and Digital Audio, Providing Advertisers with a Direct Path to Premium Inventory*, MAGNITE (Jan. 9, 2024), https://investor.magnite.com/news-releases/news-release-details/iheartmedia-and-magnite-unify-access-broadcast-and-digital audio.

87. It is estimated that Magnite collects information on a billion website interactions. "By leveraging [its] platform, [Magnite] believe[s] buyers can reach approximately one billion internet users globally, including through many of the world's largest and most premium sellers."[47]

88. Magnite calls its suite of identity resolution products the Magnite Access Suite.[48]

89. Magnite's suite includes four products: Magnite DMP; Magnite Storefront; Magnite Match; and Magnite Audiences.[49]

90. Magnite DMP helps publishers sell their first-party data. It "enables sellers to seamlessly create, [audience] segment[s]" so they can make their data more valuable to buyers.[50]

91. Magnite Storefront "enables the activation of buyer and seller first-party data on the sell side and facilitates the buying and selling of third-party data–from discovery to activation–across all of Magnite's platforms."[51]

92. Magnite Match is "a cloud-based solution that allows sellers and buyers to establish a match between data sets" so that a publisher's first-party data can be merged and enhanced with other data about the same individual.[52]

93. Magnite Audiences are "cross-publisher segments that Magnite packages to make it easier and more efficient for buyers to reach high value audiences at scale."[53] In other words, Magnite takes a publisher's first-party data and combines it with first-party data from other publishers where the individuals have similar interests based on their web activity, which "generates a potential new revenue stream for publishers with no additional operational overhead."[54]

[47] MAGNITE FORM 10-K, at 9 (2016), https://investor.magnite.com/static-files/88921618-9e64-4b6b-9bb1-ef1422015f44.

[48] *Introducing Magnite Access: An Omnichannel Audience, Data and Identity Suite*, MAGNITE (June 15, 2023), https://www.magnite.com/press/introducing-magnite-access-an-omnichannel-audience-data-and-identity-suite/.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.*

* * *

94. This is a non-exhaustive list of the entities with whom Microsoft syncs its user cookies on Defendant's Website. Suffice it to say, Microsoft is syncing its user cookies with numerous data brokers like PubMatic and Magnite to collect as much information about a user as possible and deanonymize the user, all of which is used for advertising purposes that enrich the Third Parties and Defendant alike.

95. The ADNXS Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 684 F. Supp. 3d at 1050; *Lesh*, 767 F. Supp. 3d at 40 (quoting same).

96. Further, the ADNXS Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *See*, *e.g.*, *James v. Walt Disney Co.,* 701 F. Supp. 3d 942, 958 (N.D. Cal. 2023), *motion to certify appeal denied*, 2024 WL 664811 (N.D. Cal. Feb. 16, 2024); *Lesh*, 767 F. Supp. 3d at 40 (quoting same).

97. Because the ADNXS Tracker captures outgoing "routing, addressing, and signaling" information—the IP address, Device Metadata, and unique user IDs—from visitors to the Website, it is a "pen register" for the purposes of CIPA § 638.50(b).

98. The ADNXS Tracker is also a "pen register" because the information it records is being used to ascertain the identity of visitors to Defendant's Website and is thus recording "addressing" information. *Greenley*, 684 F. Supp. 3d at 1050 ("software that identifies consumers" is a pen register).

2. The OpenX Tracker

99. Defendant incorporates the OpenX Tracker's code into the code of its Website, including when Plaintiff and Class Members visited the Website. OpenX is a registered data broker in California[55] that develops and operates the OpenX Tracker, sometimes called "OpenAudience," which it provides to website owners like Defendant for a fee.

[55] *Data Broker Registration for OpenX Technologies, Inc.*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-broker/registration/193614.

100. OpenX helps companies like Defendant "utilize their [first party] data, leverage [third party data], and package up audiences for marketers that will drive ad revenue."[56]

101. OpenX takes this data and uses it to "match [a company's] audience against [OpenX's] graph to put users in audience segments that [OpenX] mak[es] available to marketers."[57]

102. In other words, OpenX compiles comprehensive user profiles by tracking users across the Internet. OpenX then augments the information of its client's end users (like Defendant's end users) with the profile data to make that information more valuable to advertisers by aggregating that information into a graph, thereby driving Defendant's revenue. To achieve this, OpenX uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors to Defendant's Website.

103. The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the OpenX on the user's browser. The OpenX Tracker, in turn, instructs the user's browser to send OpenX the user's IP address and Device Metadata—which OpenX records through its Tracker—as the below screenshot from Plaintiff Yee's browser on the Website indicates (relevant portions in red boxes).

//

//

//

//

//

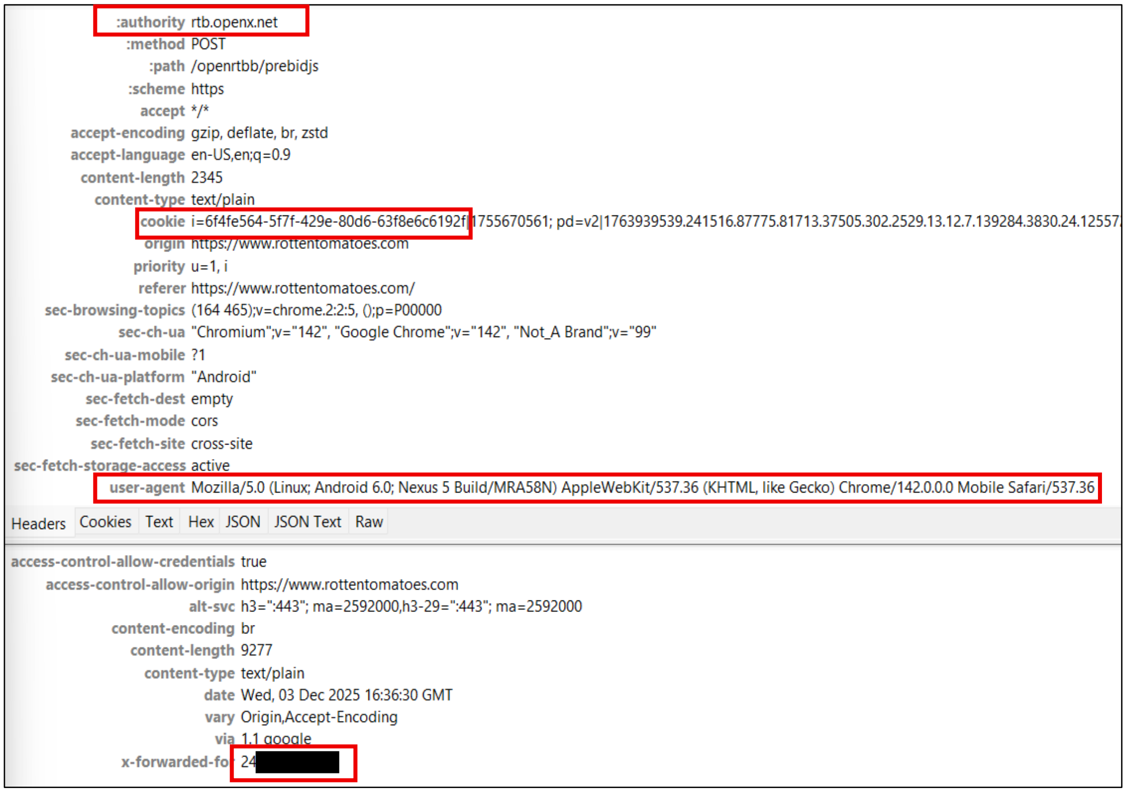
//

//

[56] *OpenAudience*, OpenX, https://www.openx.com/why-openx/openaudience/ (last accessed Jan. 27, 2025). First-party data is data that websites "collect directly from [their] customers," while third-party data is data that is "acquire[d] from a data aggregator" that does "not collect data directly but obtain[s] it from other companies and compile[s] it into a single dataset." What is the Difference Between First-Party, Second-Party and Third-Party Data?, Customer Data Platform Resource, https://tinyurl.com/2htc6a8n.

[57] *Data Activation*, OpenX, https://www.openx.com/why-openx/openaudience/.

Figure 8:



```
               :authority rtb.openx.net
                  :method POST
                    :path /openrtbb/prebidjs
                  :scheme https
                   accept */*
          accept-encoding gzip, deflate, br, zstd
          accept-language en-US,en;q=0.9
           content-length 2345
             content-type text/plain
                   cookie i=6f4fe564-5f7f-429e-80d6-63f8e6c6192f|1755670561; pd=v2|1763939539.241516.87775.81713.37505.302.2529.13.12.7.139284.3830.24.12557
                   origin https://www.rottentomatoes.com
                 priority u=1, i
                  referer https://www.rottentomatoes.com/
       sec-browsing-topics (164 465);v=chrome.2:2:5, ();p=P00000
                sec-ch-ua "Chromium";v="142", "Google Chrome";v="142", "Not_A Brand";v="99"
         sec-ch-ua-mobile ?1
       sec-ch-ua-platform "Android"
           sec-fetch-dest empty
           sec-fetch-mode cors
           sec-fetch-site cross-site
  sec-fetch-storage-access active
               user-agent Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Mobile Safari/537.36
```

```
access-control-allow-credentials true
     access-control-allow-origin https://www.rottentomatoes.com
                         alt-svc h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
                content-encoding br
                  content-length 9277
                    content-type text/plain
                            date Wed, 03 Dec 2025 16:36:30 GMT
                            vary Origin,Accept-Encoding
                             via 1.1 google
                  x-forwarded-fo 24[redacted]
```

104. Moreover, as shown above, OpenX stores a cookie with the user's IP address and Device Metadata in the user's browser cache (the unique identifier, "i"). When the user subsequently visits Defendant's Website, the OpenX Tracker locates the cookie identifier stored on the user's browser. If the cookie is stored on the browser, the OpenX Tracker causes the browser to send the cookie along with the user's IP address and Device Metadata to OpenX. A general diagram of this process is pictured as Figure 5, which explains how the Website causes the OpenX Tracker to install a cookie on the user's browser and instructs the user's browser to send the user's IP address and Device Metadata through the cookie.

105. If the user clears his or her cookies, then the user wipes out the OpenX Tracker from his or her cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the OpenX Tracker on the user's browser, (ii) the OpenX Tracker instructs the browser to send OpenX the user's IP address and Device Metadata, (iii) the OpenX Tracker stores a cookie in the browser cache, and (iv) OpenX will continue to receive the

user's IP address and Device Metadata on subsequent visits to the Website as part of the cookie transmission.

106. In all cases, however, OpenX receives a user's IP address, Device Metadata, and unique user identifier every time its Tracker is loaded by the Website, as the above screenshots indicate.

107. The OpenX Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 684 F. Supp. 3d at 1050; *Lesh*, 767 F. Supp. 3d at 40 (quoting same).

108. Further, the OpenX Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *See*, *e.g.*, *James*, 701 F. Supp. 3d at 958; *Lesh*, 767 F. Supp. 3d at 40 (quoting same).

109. Because the OpenX Tracker captures outgoing "routing, addressing, and signaling" information—the IP address, Device Metadata, and unique user IDs—from visitors to the Website, it is a "pen register" for the purposes of CIPA § 638.50(b).

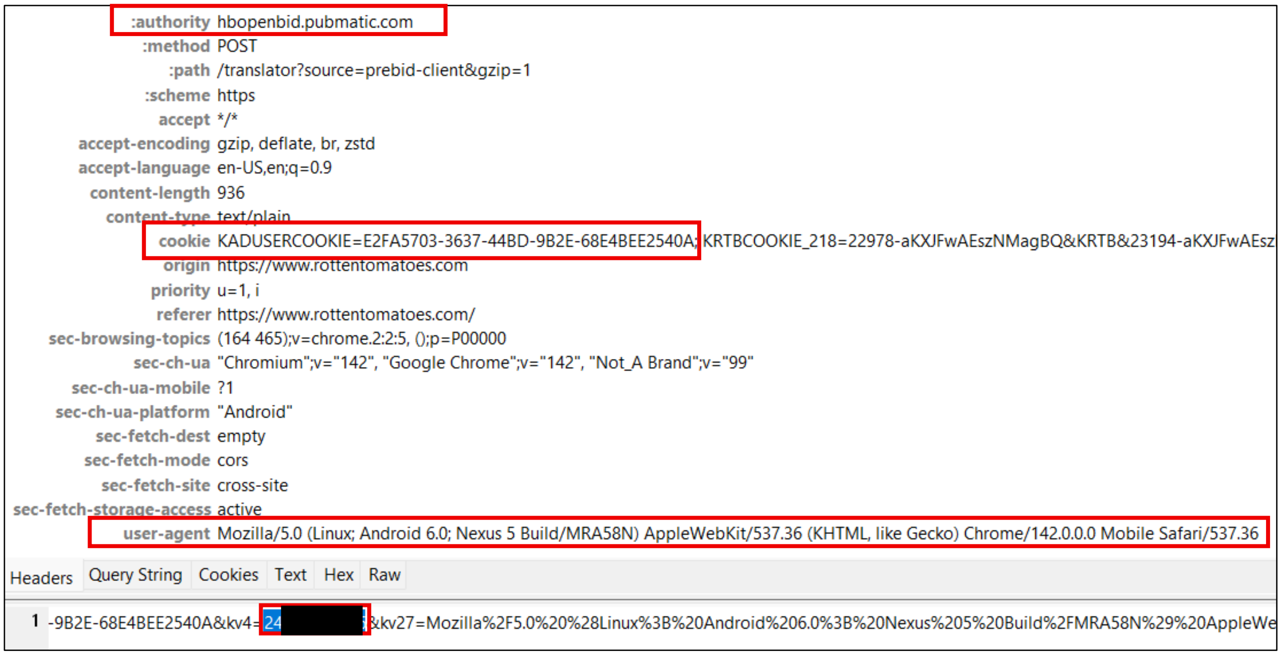
110. The OpenX Tracker is also a "pen register" because the information it records is being used to ascertain the identity of visitors to Defendant's Website and is thus recording "addressing" information. *Greenley*, 684 F. Supp. 3d at 1050 ("software that identifies consumers" is a pen register).

3. The PubMatic Tracker And The Data Brokers It Cookie-Syncs With on the Website

111. As described above, PubMatic uses its PubMatic Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

112. The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the PubMatic Tracker on the user's browser. The PubMatic Tracker, in turn, instructs the user's browser to send PubMatic the user's IP address and Device Metadata—which PubMatic records through its Tracker—as the below screenshot from Plaintiff Yee's browser on the Website indicates (relevant portions highlighted in red boxes and IP address highlighted in blue).

Figure 9:



```
           :authority hbopenbid.pubmatic.com
              :method POST
                :path /translator?source=prebid-client&gzip=1
              :scheme https
               accept */*
      accept-encoding gzip, deflate, br, zstd
      accept-language en-US,en;q=0.9
       content-length 936
         content-type text/plain
               cookie KADUSERCOOKIE=E2FA5703-3637-44BD-9B2E-68E4BEE2540A; KRTBCOOKIE_218=22978-aKXJFwAEszNMagBQ&KRTB&23194-aKXJFwAEsz
               origin https://www.rottentomatoes.com
             priority u=1, i
              referer https://www.rottentomatoes.com/
   sec-browsing-topics (164 465);v=chrome.2:2:5, ();p=P00000
            sec-ch-ua "Chromium";v="142", "Google Chrome";v="142", "Not_A Brand";v="99"
     sec-ch-ua-mobile ?1
   sec-ch-ua-platform "Android"
       sec-fetch-dest empty
       sec-fetch-mode cors
       sec-fetch-site cross-site
sec-fetch-storage-access active
           user-agent Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Mobile Safari/537.36
```

Headers Query String Cookies Text Hex Raw

```
1 -9B2E-68E4BEE2540A&kv4=[redacted]&kv27=Mozilla%2F5.0%20%28Linux%3B%20Android%206.0%3B%20Nexus%205%20Build%2FMRA58N%29%20AppleWe
```

113. Indeed, as PubMatic admits, its Tracker "automatically collects" "Browser and Device Information, such as the IP address you use to connect to an online service; device type and model; manufacturer; operating system type and version (e.g. iOS or Android); web browser type and version (e.g., Chrome or Safari); user-agent; carrier name; time zone; network connection type (e.g., Wi-Fi or cellular); and information about our Publisher's apps and versions currently active on a device."[58]

114. The PubMatic Tracker also set PubMatic's KADUSERCOOKIE on Plaintiff's browser. The KADUSERCOOKIE is specifically used to "uniquely identify each browser or device from which an individual user visits our partners' websites."[59]

115. If the user clears his or her cookies, then the user wipes out the PubMatic Tracker from its cache. Accordingly, the next time the user visits Defendant's Website, the process begins over again: (i) Defendant's server installs the PubMatic Tracker on the user's browser, (ii) the PubMatic Tracker instructs the browser to send PubMatic the user's IP address and Device Metadata,

[58] ADVERTISER PLATFORM PRIVACY POLICY, https://pubmatic.com/legal/privacy-policy/#userinfowecollect

[59] PLATFORM COOKIE & OTHER SIMILAR TECHNOLOGIES POLICY, https://pubmatic.com/legal/platform-cookie-policy/

(iii) the PubMatic Tracker stores the unique KADUSERCOOKIE identifier in the browser cache, and (iv) PubMatic will continue to receive the user's IP address and Device Metadata on subsequent Website visits along with the KADUSERCOOKIE.

116. In all cases, however, PubMatic receives a user's IP address, Device Metadata, and unique user identifier every time its Tracker is loaded by the Website, as the above screenshots indicate.

117. PubMatic is also syncing its unique user identifier with ID5 Technology,[60] Tapad, Inc.[61]/Experian Information Solutions, Inc.,[62] and Sovrn/Lijit,[63] all of which are registered data brokers in California.

(i) ID5 ID Tracker

118. For example, PubMatic syncs the KADUSERCOOKIE value with the ID5 ID Tracker owned by ID5 Technology—as the below screenshot from Plaintiff Yee's browser on the Website indicates (relevant portions highlighted in red boxes):

//

//

//

//

//

//

//

//

//

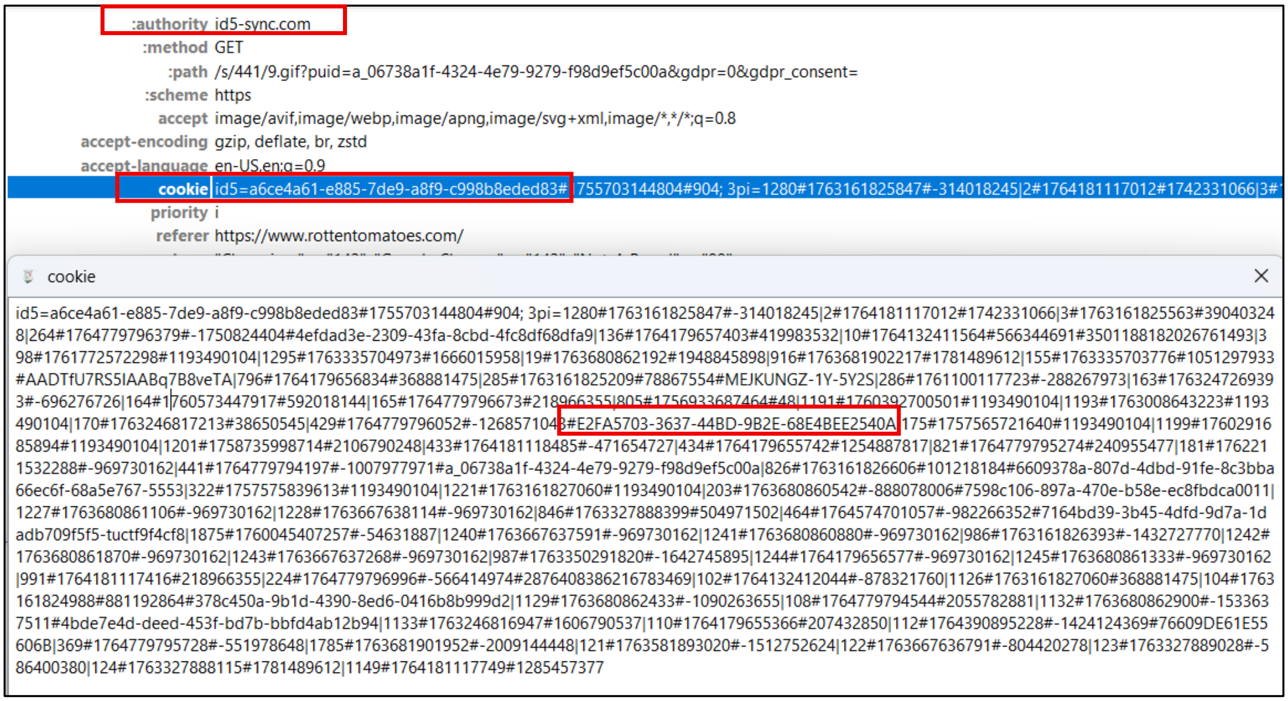
[60] *Data Broker Registration, for ID5 Technology*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-broker/registration/550584.

[61] *Data Broker Registration, for Tapad, Inc.*, OFFICE OF THE ATTORNEY GENERAL, HTTPS://OAG.CA.GOV/DATA-BROKER/REGISTRATION/187511.

[62] *Data Broker Registration, for Tapad, Inc.*, OFFICE OF THE ATTORNEY GENERAL, HTTPS://OAG.CA.GOV/DATA-BROKER/REGISTRATION/186691.

[63] *Data Broker Registration, for Sovrn, Inc.*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-brokers?page=15.

Figure 10:



```
      :authority id5-sync.com
         :method GET
           :path /s/441/9.gif?puid=a_06738a1f-4324-4e79-9279-f98d9ef5c00a&gdpr=0&gdpr_consent=
         :scheme https
          accept image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
 accept-encoding gzip, deflate, br, zstd
 accept-language en-US,en;q=0.9
          cookie id5=a6ce4a61-e885-7de9-a8f9-c998b8eded83#1755703144804#904; 3pi=1280#1763161825847#-314018245|2#1764181117012#1742331066|3#
        priority i
         referer https://www.rottentomatoes.com/
```

cookie

```
id5=a6ce4a61-e885-7de9-a8f9-c998b8eded83#1755703144804#904; 3pi=1280#1763161825847#-314018245|2#1764181117012#1742331066|3#1763161825563#39040324
8|264#1764779796379#-1750824404#4efdad3e-2309-43fa-8cbd-4fc8df68dfa9|136#1764179657403#419983532|10#1764132411564#566344691#3501188182026761493|3
98#1761772572298#1193490104|1295#1763335704973#1666015958|19#1763680862192#1948845898|916#1763681902217#1781489612|155#1763335703776#1051297933
#AADTfU7RS5IAABq7B8veTA|796#1764179656834#368881475|285#1763161825209#78867554#MEJKUNGZ-1Y-5Y2S|286#1761100117723#-288267973|163#176324726939
3#-696276726|164#1760573447917#592018144|165#1764779796673#218966355|805#1756933687464#48|1191#1760392700501#1193490104|1193#1763008643223#1193
490104|170#1763246817213#38650545|429#1764779796052#-1268571043#E2FA5703-3637-44BD-9B2E-68E4BEE2540A|175#1757565721640#1193490104|1199#17602916
85894#1193490104|1201#1758735998714#2106790248|433#1764181118485#-471654727|434#1764179655742#1254887817|821#1764779795274#240955477|181#176221
1532288#-969730162|441#1764779794197#-1007977971#a_06738a1f-4324-4e79-9279-f98d9ef5c00a|826#1763161826606#101218184#6609378a-807d-4dbd-91fe-8c3bba
66ec6f-68a5e767-5553|322#1757575839613#1193490104|1221#1763161827060#1193490104|203#1763680860542#-888078006#7598c106-897a-470e-b58e-ec8fbdca0011|
1227#1763680861106#-969730162|1228#1763667638114#-969730162|846#1763327888399#504971502|464#1764574701057#-982266352#7164bd39-3b45-4dfd-9d7a-1d
adb709f5f5-tuctf9f4cf8|1875#1760045407257#-54631887|1240#1763667637591#-969730162|1241#1763680860880#-969730162|986#1763161826393#-1432727770|1242#
1763680861870#-969730162|1243#1763667637268#-969730162|987#1763350291820#-1642745895|1244#1764179656577#-969730162|1245#1763680861333#-969730162
|991#1764181117416#218966355|224#1764779796996#-566414974#2876408386216783469|102#1764132412044#-878321760|1126#1763161827060#368881475|104#1763
161824988#881192864#378c450a-9b1d-4390-8ed6-0416b8b999d2|1129#1763680862433#-1090263655|108#1764779794544#2055782881|1132#1763680862900#-153363
7511#4bde7e4d-deed-453f-bd7b-bbfd4ab12b94|1133#1763246816947#1606790537|110#1764179655366#207432850|112#1764390895228#-1424124369#76609DE61E55
606B|369#1764779795728#-551978648|1785#1763681901952#-2009144448|121#1763581893020#-1512752624|122#1763667636791#-804420278|123#1763327889028#-5
86400380|124#1763327888115#1781489612|1149#1764181117749#1285457377
```

119. This allows PubMatic to obtain whatever information ID5 has on the user (and vice versa). Indeed, the "id5-sync.com" value leaves little doubt that PubMatic is matching its cookies with ID5 to obtain any information ID5 has about Plaintiff Yee (and vice versa). ID5 also enhances the information PubMatic knows about Plaintiff Yee with information that ID5 knows about Plaintiff. Finally, ID5 enhances this user information by installing its own cookie on Plaintiff Yee's browser for further tracking, syncing, and de-anonymization.

120. ID5 boasts that its "ID5 ID" "is a next-generation universal identifier that publishers, advertisers and ad tech platforms can use to recognise users and deliver campaign objectives across different types of devices without relying on traditional identification methods (e.g. third-party cookies and MAIDs)."[64] It helps website owners like Defendant utilize their first party data by "leveraging a variety of signals such as hashed email addresses, page URL, IP addresses, timestamps

[64] ID5, https://github.com/id5io/id5-api.js/blob/master/README.md; *see also*, *First-party IDs and identity resolution methods explained,* ID5, (March 23, 2022), https://id5.io/news/first-party-ids-and-identity-resolution-methods-explained (ID5 uses "hashed email addresses and IP addresses" to "reconcile users across domains and devices.").

etc., as well as a machine learning algorithm" to package up audiences for marketers that will drive ad revenue.[65] It does this with "IdentityCloud," its comprehensive suite of services.[66]

121. According to ID5, it "provides an evolving suite of identity solutions for the digital advertising ecosystem" to "enable[e] effective advertising. [Its] technology platform enables publishers and advertisers to more effectively recognize browsers and other devices over time by generating a unique, pseudonymous ID."[67] This helps website owners like Defendant recognize users and target them for advertisements.

122. ID5's "Adaptive Identity" technology is "designed to solve identity challenges at scale in a fragmented ecosystem. At its core is machine learning, which allows [ID5] to move beyond rigid rules and one-size-fits-all approaches. Instead of relying on static logics, Adaptive Identity continuously learns from behavioral patterns, environments, and outcomes, making identity resolution smarter, more accurate, and more resilient over time."[68] It can follow website users "across channels, across devices, and across the ecosystem."[69]

123. Recently, ID5 augmented these capabilities by acquiring "TrueData, an identity resolution provider that connects people and households to their digital devices."[70] ID5 touts that it "will combine its cross-device ID system and graph with TrueData's identity graph and online and offline data assets, including retail transaction information, IP addresses, connected TV identifiers, hashed emails, mobile IDs and other probabilistic IDs," to "recognize roughly 1.5 billion users across 665 million households."[71]

[65] ID5, https://github.com/id5io/id5-api.js/blob/master/README.md

[66] *ID5 Launches IdentityCloud, the Comprehensive Identity Solution for Digital Advertising*, EXCHANGEWIRE (Oct. 21, 2021), https://www.exchangewire.com/blog/2021/10/21/id5-launches-identitycloud-comprehensive-identity-solution/.

[67] ID5, https://id5.io/platform-privacy-policy/.

[68] ID5, https://id5.io/news/introducing-adaptive-identity-a-smarter-approach-to-addressability-for-a-connected-world.

[69] *Id.*

[70] https://www.adexchanger.com/identity/alt-identity-provider-id5-buys-truedata-marking-its-first-ever-acquisition/

[71] *Id.*

124. The upshot of all this is that ID5 enables website owners like Defendant to effectively sell their user inventory to advertisers in a de-anonymized, targeted format. By syncing its tracker with PubMatic's, ID5 facilitates this goal, leveraging PubMatic's replete database of user profiles to de-anonymize and identify Website users.

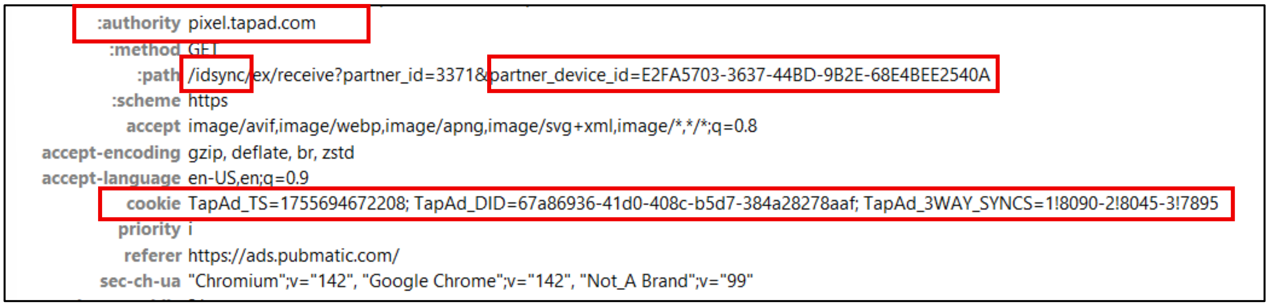
125. PubMatic, in turn, builds on its already expansive database by learning whatever ID5 knows about the Website user. And Defendant profits from installing both trackers on its Website because its users can be sold to advertisers for more money, thus enriching Defendant.

(ii) Tapad/Experian Tracker

126. As another example, PubMatic syncs its KADUSERCOOKIE value with the Tapad tracker which Defendant also installs on the browsers of visitors to the Website.

127. As the screenshot below from Plaintiff's browser indicates, the value of the "partner_device_id" parameter matches the value of the KADUSERCOOKIE parameter above. Tapad is also enhancing the information PubMatic knows about Plaintiff with information that Tapad knows about Plaintiff (and vice versa), something indicated by the path of the GET request, "idsync." Finally, Tapad is installing its own cookies on Plaintiff's browser for further tracking, syncing, and de-anonymization.

Figure 11:



```
       :authority pixel.tapad.com
          :method GET
            :path /idsync/ex/receive?partner_id=3371&partner_device_id=E2FA5703-3637-44BD-9B2E-68E4BEE2540A
          :scheme https
           accept image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
  accept-encoding gzip, deflate, br, zstd
  accept-language en-US,en;q=0.9
           cookie TapAd_TS=1755694672208; TapAd_DID=67a86936-41d0-408c-b5d7-384a28278aaf; TapAd_3WAY_SYNCS=1!8090-2!8045-3!7895
         priority i
          referer https://ads.pubmatic.com/
        sec-ch-ua "Chromium";v="142", "Google Chrome";v="142", "Not_A Brand";v="99"
```

128. As mentioned previously, Tapad is a registered data broker in California and is owned and operated by Experian,[72] another registered data broker.

129. The purpose of Tapad's tracker—which is used is in conjunction with Experian's services—is to perform identity resolution. As Experian describes it:

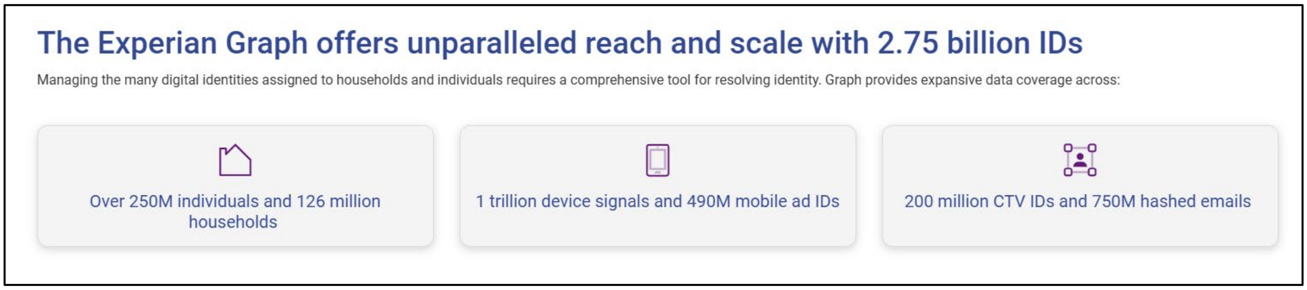
[72] Allison Schiff, *Telenor Sells Tapad to Experian for $280 Million*, ADEXCHANGER (Nov. 19, 2020), https://www.adexchanger.com/privacy/telenor-sells-Tapad-to-experian-for-280-million/.

> [i]dentity resolution matches fragmented identifiers to a single profile. This creates a unified, cross-channel view of a consumer that helps marketers understand a customer's demographics, lifestyle, interests, and where and how they engage with your brand. Identity resolution improves campaign targeting and enables marketers to deliver personalized marketing messages.[73]

130. Tapad identifies users by "crunching 150 billion data points—from cookies, cellphone IDs (which link individual phones to app downloads and Web browsing), Wi-Fi connections, website registrations, browsing history and other inputs."[74] Tapad then aggregates these inputs into what it called a "Device Graph," which allows advertisers to connect individuals to all the devices those individuals use for the purpose of delivering targeted advertisements.[75]

131. Tapad integrates with Experian's "offline consumer data set (purchase behaviors, interests, lifestyle info)."[76] This includes "first-party data such as names, physical addresses, email addresses, mobile ad identifiers (MAIDs), IP addresses, and other information."[77] And as Experian advertisers, its identity graph is composed of "[o]ver 250M individuals and 126 million households," enabling its partners like Microsoft to "known and anonymous IDs and data back to a single person or household to resolve identity."[78]

Figure 12:



The Experian Graph offers unparalleled reach and scale with 2.75 billion IDs

Managing the many digital identities assigned to households and individuals requires a comprehensive tool for resolving identity. Graph provides expansive data coverage across:

Over 250M individuals and 126 million households

1 trillion device signals and 490M mobile ad IDs

200 million CTV IDs and 750M hashed emails

[73] Identity Resolution Solutions, https://www.experian.com/marketing/consumer-sync/identity-resolution.

[74] *Id.*

[75] Ingrid Lunden, *Telenor Jumps Into Ad Tech, Acquires Tapad For $360M*, TechCrunch (Feb. 1, 2016), https://techcrunch.com/2016/02/01/telenor-jumps-into-ad-tech-acquires-Tapad-for-360m/.

[76] Anthony Vargas, *How Experian Is Using Tapad To Build New ID Resolution And Analytics Products*, ADEXCHANGER (Feb. 1, 2023), https://www.adexchanger.com/data-exchanges/how-experian-is-using-tapad-to-build-new-id-resolution-and-analytics-products/.

[77] Sherman, *supra*, at 6 (cleaned up); *see also* Experian, OmniImpact, https://tinyurl.com/mve5jb65.

[78] Graph | Experian's Identity Graph, https://www.experian.com/marketing/consumer-sync/identity-resolution/identity-graph.

132. Thus, when PubMatic solicits bids from advertisers for users' information—as is the PubMatic Tracker's function as a supply-side platform—advertisers can better identify and target their bids as a result of the PubMatic Tracker syncing with Tapad's tracker, which de-anonymizes and identifies users. Tapad and Experian, in turn, build on their already expansive database through this transaction. And Defendant profits from installing both trackers on its Website because its users can be sold to advertisers for more money, thus enriching Defendant.

(iii) <u>The Lijit/Sovrn Tracker</u>

133. PubMatic also syncs the KADUSERCOOKIE value with the Lijit Tracker which is also installed by Defendant on the Website.

134. As pictured in the below screenshot from Plaintiff's browser on the Website, the value of the "_ljtrtb_58" parameter matches the value of the KADUSERCOOKIE parameter in Figure 13 above. This allows PubMatic to obtain whatever information Lijit has on the user (and vice versa). Indeed, Lijit admits that each "_ljtrtb_[Partner ID]" identifier is "consolidate[d] … into the ljtrtb cookie when it's available," that the "ljtrtb" identifier "[e]nables us to help our advertising partners make decisions about displaying an advertisement to you," and that the "lijitrtb" identifier "store[s] the ID that each partner uses to identify you and pass that information to the partner when a website requests an advertisement from us."[79] Lijit also installed the "ljtrtb" cookie on Plaintiff's browser, as well as the "ljt_reader" cookie, which "[e]nables us to recognize your browser or device when you return to our site or one of our partner's sites."[80]

//

//

//

//

//

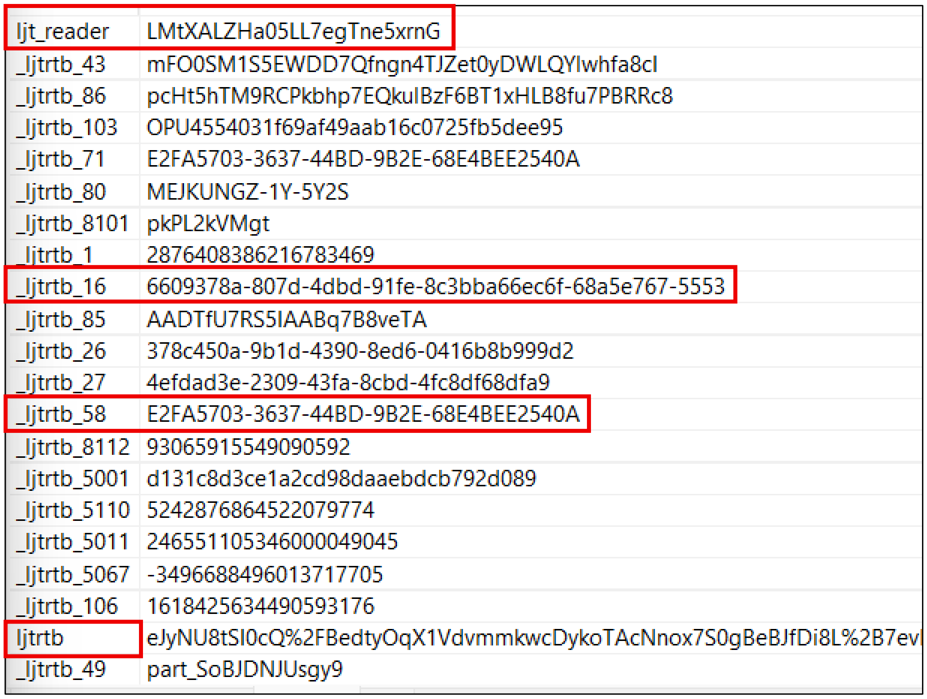
//

//

[79] SOVRN WEBSITE COOKIES, SOVRN, https://www.sovrn.com/about-our-cookies/.

[80] *Id.*

Figure 13:



ljt_reader	LMtXALZHa05LL7egTne5xrnG
_ljtrtb_43	mFO0SM1S5EWDD7Qfngn4TJZet0yDWLQYlwhfa8cl
_ljtrtb_86	pcHt5hTM9RCPkbhp7EQkulBzF6BT1xHLB8fu7PBRRc8
_ljtrtb_103	OPU4554031f69af49aab16c0725fb5dee95
_ljtrtb_71	E2FA5703-3637-44BD-9B2E-68E4BEE2540A
_ljtrtb_80	MEJKUNGZ-1Y-5Y2S
_ljtrtb_8101	pkPL2kVMgt
_ljtrtb_1	2876408386216783469
_ljtrtb_16	6609378a-807d-4dbd-91fe-8c3bba66ec6f-68a5e767-5553
_ljtrtb_85	AADTfU7RS5IAABq7B8veTA
_ljtrtb_26	378c450a-9b1d-4390-8ed6-0416b8b999d2
_ljtrtb_27	4efdad3e-2309-43fa-8cbd-4fc8df68dfa9
_ljtrtb_58	E2FA5703-3637-44BD-9B2E-68E4BEE2540A
_ljtrtb_8112	93065915549090592
_ljtrtb_5001	d131c8d3ce1a2cd98daaebdcb792d089
_ljtrtb_5110	5242876864522079774
_ljtrtb_5011	246551105346000049045
_ljtrtb_5067	-3496688496013717705
_ljtrtb_106	1618425634490593176
ljtrtb	eJyNU8tSI0cQ%2FBedtyOqX1VdvmmkwcDykoTAcNnox7S0gBeBJfDi8L%2B7ev
_ljtrtb_49	part_SoBJDNJUsgy9

135. The long and short of this process is that Lijit shares whatever information Lijit has—and that Lijit gains by syncing with a variety of partners—with PubMatic (and vice versa), enabling Plaintiff to be tracked, identified, and de-anonymized. And as the partner IDs in the above screenshot indicate, Lijit is syncing its cookie with numerous data brokers whose trackers Defendant also installs on the Website, and all of that information is being shared between Lijit and each of its partners. By way of example, the value of "_ljtrtb_16" in Figure 13 above corresponds to an identifier that Lijit syncs with Tapad (and thus, has Tapad sync its information with Lijit and each of its partners). Tapad's functionalities and status as a data broker are described above.

136. Sovrn operates as an SSP, although it provides additional features.[81] Sovrn leverages is relationships "with all of the top supply-side platforms" to "negotiate better 'take rates' with these exchanges than the typical publisher [*i.e.*, a website operator like Defendant] could get on their own," allowing website operators like Defendant who install Sovrn's tracker on their website "to earn more revenue from the start."[82]

[81] WHAT WE DO, SOVRN, https://www.sovrn.com/about-sovrn/.

[82] Sovrn Publisher Advocate, *Make More, Keep More*, SOVRN (Feb. 17, 2022), https://www.sovrn.com/blog/make-more-keep-more/.

137. Sovrn achieves this by running a "single unified auction" that enables the servicing of an advertisement (by selling consumer data to advertisers) to "[t]he three highest bids on the page."[83]

138. For individuals who visit websites like Defendant's where Sovrn's tracker is installed, it "set[s] cookies (where allowed) at the first visit to any of the Publisher sites that deploy Sovrn Services. If our cookie is already set on a browser, we recognize a returning Reader and log data using the existing cookie." [84]

139. With the information gathered with the cookies, Sovrn creates user profiles for users, or "audience segments," as Sovrn refers to them, "by categorizing Personal Information we have collected by common interests, intent or other characteristics. … Audience segments are used to provide additional insights, enrichment of our Publisher's first party data, and to attribute reader interests to browsers and devices to better inform advertising campaigns.[85]

140. Indeed, Sovrn touts it provides website operators like Defendant with access to the "Sovrn Data Collective," "the world's largest publisher collective for deep consumer insights and enriched audience data."[86]

141. One of the reasons Sovrn is so successful at monetizing information is because it matches user's information to their hashed e-mail address. As Sovrn notes, "[t]he Sovrn Hashed Email solution creates an additional revenue stream for publishers allowing them to monetize their data … with increased CPMs."[87]

142. Indeed, the below screenshot shows that Sovrn has a unique identifier correspodening to Plaintiff's e-mail address in various "hashed" formats (md5, sha1, sha256), which shares with each of the trackers it syncs with like PubMatic.

[83] *Id.*

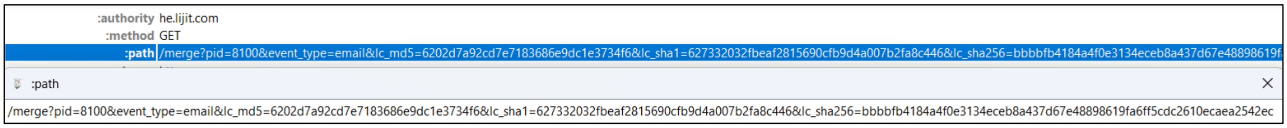
[84] SOVRN SERVER TO SERVER BIDDING & OPENRTB INTEGRATION GUIDE, https://knowledge.sovrn.com/kb/sovrn-server-to-server-bidding-openrtb-integration.

[85] SOVRN PRIVACY POLICY, https://www.sovrn.com/privacy-policy/privacy-policy/.

[86] DATA MONETIZATION, SOVRN, https://www.sovrn.com/data-monetization/.

[87] DATA PRODUCTS: EMAIL MONETIZATION OVERVIEW, https://knowledge.sovrn.com/kb/data-products-email-monetization-overview.

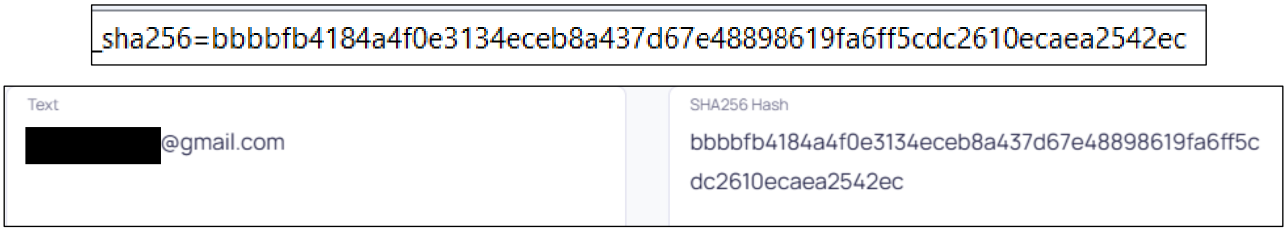
Figure 14:



```
:authority he.lijit.com
   :method GET
     :path /merge?pid=8100&event_type=email&lc_md5=6202d7a92cd7e7183686e9dc1e3734f6&lc_sha1=627332032fbeaf2815690cfb9d4a007b2fa8c446&lc_sha256=bbbbfb4184a4f0e3134eceb8a437d67e48898619f
:path
/merge?pid=8100&event_type=email&lc_md5=6202d7a92cd7e7183686e9dc1e3734f6&lc_sha1=627332032fbeaf2815690cfb9d4a007b2fa8c446&lc_sha256=bbbbfb4184a4f0e3134eceb8a437d67e48898619fa6ff5cdc2610ecaea2542ec
```

143. To illustrate this is Plaintiff's e-mail address, putting Plaintiff's e-mail address into a sha256 encoder/decoder[88] yields the same "sha256" value as in Figure 14 (reproduced below):

Figure 15:



sha256=bbbbfb4184a4f0e3134eceb8a437d67e48898619fa6ff5cdc2610ecaea2542ec

Text

[redacted]@gmail.com

SHA256 Hash

bbbbfb4184a4f0e3134eceb8a437d67e48898619fa6ff5cdc2610ecaea2542ec

144. Although hashing is ostensibly "privacy protective," e-mail addresses are still traceable in hashed form to individuals. As the FTC has noted multiple times, "hashes aren't 'anonymous' and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized."[89] Indeed, "the casual assumption that hashing is sufficient to anonymize data is risky at best, and usually wrong."[90]

145. Thus, what Sovrn is doing is collecting and maintaining a database of e-mails, enriching that information by syncing its trackers with those of data brokers (*e.g.*, Tapad) and sharing all that information with PubMatic and other third parties whose trackers Defendant installs on its Website, all of which is intended to enrich Defendant.

* * *

146. This is a non-exhaustive list of the entities with whom PubMatic syncs its user cookies on Defendant's Website. PubMatic is syncing its user cookies with numerous data brokers like ID5, Sovrn/Lijit, and Experian/Tapad to collect as much information about a user as possible and

[88] *See*, *e.g.*, https://10015.io/tools/sha256-encrypt-decrypt/.

[89] *No, Hashing Still Doesn't Making Your Data Anonymous*, Federal Trade Commission (July 24, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous.

[90] Ed Felten, *Does Hashing Make Data "Anonymous"?*, FEDERAL TRADE COMMISSION (Apr. 22, 2012), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous.

deanonymize the user, all of which is used for advertising purposes that enrich the Third Parties and Defendant alike.

147. The PubMatic Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 684 F. Supp. 3d at 1050; *Lesh*, 767 F. Supp. 3d at 40 (quoting same).

148. Further, the PubMatic Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *See*, *e.g.*, *James*, 701 F. Supp. 3d at 958; *Lesh*, 767 F. Supp. 3d at 40 (quoting same).

149. Because the PubMatic Tracker captures outgoing "routing, addressing, and signaling" information—the IP address, Device Metadata, and unique user IDs—from visitors to the Website, it is a "pen register" for the purposes of CIPA § 638.50(b).

150. The PubMatic Tracker is also a "pen register" because the information it records is being used to ascertain the identity of visitors to Defendant's Website and is thus recording "addressing" information. *Greenley*, 684 F. Supp. 3d at 1050 ("software that identifies consumers" is a pen register).

III. DEFENDANT'S CONDUCT CONSTITUTES AN INVASION OF PLAINTIFF'S AND CLASS MEMBERS' PRIVACY

151. The collection of Plaintiff's and Class Members' personally identifying deanonymized information through Defendant's installation and use of the Tracker constitutes an invasion of privacy. *See*, *e.g.*, *Deivaprakash v. Condé Nast Digital*, 798 F. Supp. 3d 1100, 1106-07, 1107 n.4 (N.D. Cal. 2025).

152. As alleged herein, the Trackers and the trackers they sync with are designed to deanonymize and identify Website users by linking various identifiers to comprehensive profiles, conduct targeted advertising, and boost Defendant's revenue, all through their surreptitious collection of Plaintiff's and Class Members' personal information.

153. To put the invasiveness of Defendant's violations of the CIPA into perspective, however, it is important to understand three concepts: data brokers, real-time bidding, and cookie syncing.

154. The import of these concepts is that: (i) the Third Parties, two of which are data brokers (OpenX and PubMatic) and Microsoft acting as a DSP, sync with other third parties that are data brokers to uniquely identify and deanonymize Website users by matching users' to their IP addresses, Device Metadata, and unique ID values with comprehensive profiles held by those data brokers (or the Third Parties themslves); (ii) the Third Parties share that information with other data brokers to create the most complete user profile they can (through cookie syncing), which includes a more complete and non-anonymous portrait of the user; and (iii) those profiles are offered up for sale through the real-time bidding process to the benefit of Defendant, the Third Parties, and the data brokers they sync with and to the detriment of users' privacy interests.

A. Data Brokers and Real-Time Bidding: The Information Economy

1. Data Brokers

155. While "[t]here is no single, agreed-upon definition of data brokers in United States law,"[91] California law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct [*i.e.*, consumer-facing] relationship," subject to certain exceptions. Cal. Civ. Code § 1798.99.80(c).

156. Any entity that qualifies as a "data broker" under California law must specifically register as such pursuant to Cal. Civ. Code § 1798.99.82(a). OpenX,[92] PubMatic,[93] Magnite,[94] ID5,[95]

[91] JUSTIN SHERMAN, DUKE SANFORD CYBER POLICY PROGRAM, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS: THREATS TO AMERICAN CIVIL RIGHTS, NATIONAL SECURITY, AND DEMOCRACY, 2 (DUKE SANFORD CYBER POLICY PROGRAM, 2021), https://tinyurl.com/hy9fewhs.

[92] *Data Broker Registration for OpenX Technologies, Inc*., OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-broker/registration/193614.

[93] *Data Broker Registration for PubMatic, Inc*., OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-broker/registration/186702.

[94] *Data Broker Registration for Magnite, Inc*., OFFICE OF THE ATTORNEY GENERAL DATA BROKER, https://oag.ca.gov/data-broker/registration/568127.

[95] *Data Broker Registration for ID5 Technology,* OFFICE OF THE ATTORNEY GENERAL DATA BROKER, https://oag.ca.gov/data-broker/registration/550584.

Tapad,[96] Experian,[97] and Sovrn[98] have registered as data brokers in California.

157. Some data brokers prefer to characterize themselves as "identity graph providers," but this is a distinction without a difference. "An identity graph provides a single unified view of customers and prospects based on their interactions with a product or website across a set of devices and identifiers. An identity graph is used for real-time personalization and advertising targeting for millions of users."[99] This is exactly what data brokers do, and indeed, the entities that provide identity graphs are by and large required to register as data brokers under California law. An "identity graph provider" is therefore just a euphemism for "data broker."

158. "Data brokers typically offer pre-packaged databases of information to potential buyers," either through the "outright s[ale of] data on individuals" or by "licens[ing] and otherwise shar[ing] the data with third parties."[100] Such databases are extensive, and can "not only include information publicly available [such as] from Facebook but also the user's exact residential address, date and year of birth, and political affiliation," in addition to "inferences [that] can be made from the combined data."[101]

159. For instance, the NATO report noted that data brokers collect two sets of information: "observed and inferred (or modelled)." The former "is data that has been collected and is actual," such as websites visited." Inferred data "is gleaned from observed data by modelling or profiling, meaning what users may be *expected* to do. On top of this, "[b]rokers typically collect not only what

[96] *Data Broker Registration for Tapad, Inc.*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-broker/registration/187511.

[97] *Data Broker Registration for Experian Information Solutions, Inc.*, OFFICE OF THE ATTORNEY GENERAL https://oag.ca.gov/data-broker/registration/186691.

[98] *Data Broker Registration for Sovrn, Inc.*, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/data-brokers?combine=sovrn.

[99] IDENTITY GRAPHS ON AWS, https://aws.amazon.com/neptune/identity-graphs-on-aws/.

[100] SHERMAN, *supra*, at 2.

[101] Tehila Minkus et al., *The City Privacy Attack: Combining Social Media and Public Records for Detailed Profiles of Adults and Children*, COSN '15: PROCEEDINGS OF THE 2015 ACM ON CONFERENCE ON ONLINE SOCIAL NETWORKS 71, 71 (2015), https://dl.acm.org/doi/pdf/10.1145/2817946.2817957.

they immediately need or can use, but hoover up as much information as possible to compile comprehensive data sets that might have some future use."[102]

160. Likewise, a report by the Duke Sanford Cyber Policy Program "examine[d] 10 major data brokers and the highly sensitive data they hold on U.S. individuals."[103] The report found that "data brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees."[104]

161. This data collection has grave implications for Americans' right to privacy. For instance, "U.S. federal agencies from the Federal Bureau of Investigation [] to U.S. Immigration and Customs Enforcement [] purchase data from data brokers—without warrants, public disclosures, or robust oversight—to carry out everything from criminal investigations to deportations."[105]

162. As another example:

> Data brokers also hold highly sensitive data on U.S. individuals such as race, ethnicity, gender, sexual orientation, immigration status, income level, and political preferences and beliefs (like support for the NAACP or National LGBTQ Task Force) that can be used to directly undermine individuals' civil rights. Even if data brokers do not explicitly advertise these types of data (though in many cases they do), everything from media reporting to testimony by a Federal Trade Commission commissioner has identified the risk that data brokers use their data sets to make "predictions" or "inferences" about this kind of sensitive information (race, gender, sexual orientation, etc.) on individuals.
>
> This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements. 59 Many industries from health insurance to life insurance to banking

[102] TWETMAN & BERGMANIS-KORATS, *supra*, at 11.

[103] SHERMAN, *supra*, at 1.

[104] *Id.*

[105] *Id.* at 9.

> to e-commerce purchase data from data brokers to run advertisements and target their services.
>
> …
>
> Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups.[106]

163. This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements.

164. Many industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services.

165. Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups.[107]

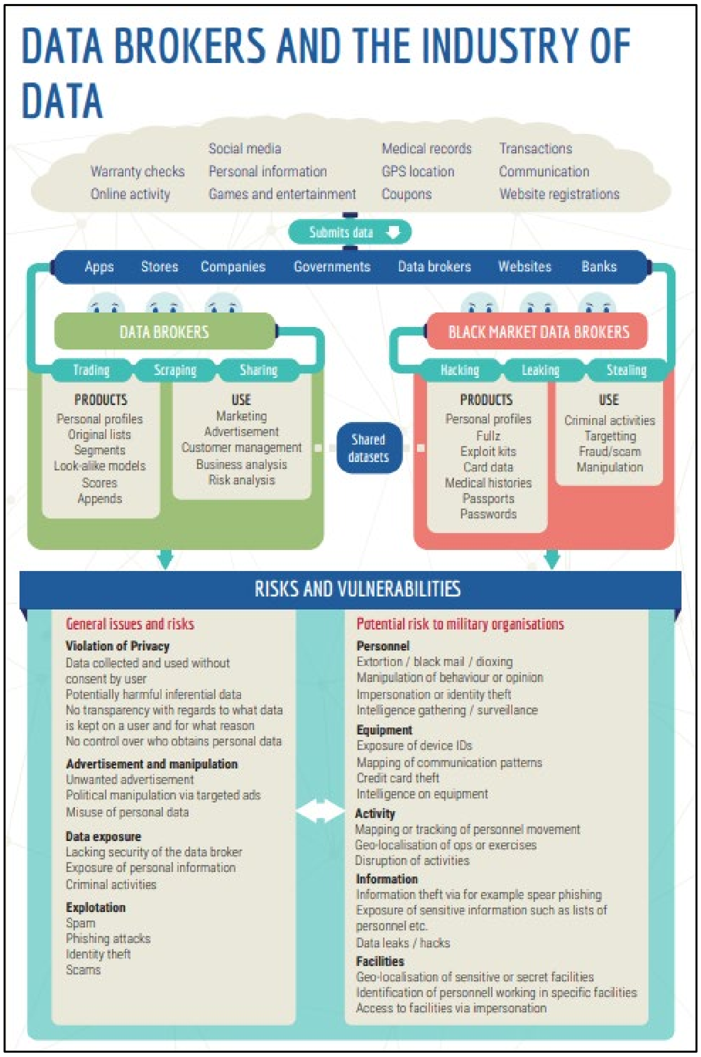
166. Similarly, as the report from NATO noted, corporate data brokers cause numerous privacy harms, including but not limited to depriving users of the right to control who does and does not acquire their personal information, unwanted advertisements that can even go as far as manipulating viewpoints, and spam and phishing attacks.[108]

[106] *Id.*

[107] *Id.*

[108] TWETMAN & BERGMANIS-KORATS, *supra*, at 8.

Figure 16:


DATA BROKERS AND THE INDUSTRY OF DATA
Warranty checks
Online activity
Social media
Personal information
Games and entertainment
Medical records
GPS location
Coupons
Transactions
Communication
Website registrations
Submits data
Apps
Stores
Companies
Governments
Data brokers
Websites
Banks
DATA BROKERS
Trading
Scraping
Sharing
PRODUCTS
Personal profiles
Original lists
Segments
Look-alike models
Scores
Appends
USE
Marketing
Advertisement
Customer management
Business analysis
Risk analysis
Shared datasets
BLACK MARKET DATA BROKERS
Hacking
Leaking
Stealing
PRODUCTS
Personal profiles
Fullz
Exploit kits
Card data
Medical histories
Passports
Passwords
USE
Criminal activities
Targetting
Fraud/scam
Manipulation
RISKS AND VULNERABILITIES
General issues and risks
Violation of Privacy
Data collected and used without consent by user
Potentially harmful inferential data
No transparency with regards to what data is kept on a user and for what reason
No control over who obtains personal data
Advertisement and manipulation
Unwanted advertisement
Political manipulation via targeted ads
Misuse of personal data
Data exposure
Lacking security of the data broker
Exposure of personal information
Criminal activities
Explotation
Spam
Phishing attacks
Identity theft
Scams
Potential risk to military organisations
Personnel
Extortion / black mail / dioxing
Manipulation of behaviour or opinion
Impersonation or identity theft
Intelligence gathering / surveillance
Equipment
Exposure of device IDs
Mapping of communication patterns
Credit card theft
Intelligence on equipment
Activity
Mapping or tracking of personnel movement
Geo-localisation of ops or exercises
Disruption of activities
Information
Information theft via for example spear phishing
Exposure of sensitive information such as lists of personnel etc.
Data leaks / hacks
Facilities
Geo-localisation of sensitive or secret facilities
Identification of personnell working in specific facilities
Access to facilities via impersonation

167. In the modern age, these threats are far too real. For instance, the gunman who assassinated a Minnesota state representative and her husband "may have gotten their addresses or other personal details from online data broker services, according to court documents."[109]

168. Similarly, following the protests in Los Angeles in the summer of 2025:

> Tech-skeptical California lawmakers and activists fear the Trump administration will leverage tech tools to track and punish demonstrators accused of interfering with Immigration and Customs Enforcement raids. One possible instrument at ICE's disposal: location data, a highly detailed record of people's daily movements

[109] Lily Hay Newman, *Minnesota Shooting Suspect Allegedly Used Data Broker Sites to Find Targets' Addresses*, WIRED (June 16, 2025), https://www.wired.com/story/minnesota-lawmaker-shootings-people-search-data-brokers/.

> that's collected and sold by everything from weather apps to data brokers.[110]

169. Of course, data brokers do not just track people for no reason; they do so because they have their trackers installed on users' browsers and are paid by website operators to do so. So, by installing so many data broker trackers on users' browsers, Defendant is causing and putting its users in the crosshairs of the privacy harms noted above.

170. In addition, as noted above, data brokers like ID5 can compile wide swaths of information in part by collecting users' IP addresses and Device Metadata, which is used by data brokers to track users across the Internet.[111]

171. As noted above, data brokers are able to compile such wide swaths of information in part by collecting users' IP addresses and Device Metadata, which are is used by data brokers to track users across the Internet.[112] Indeed, as McAfee (a data security company) notes, "data brokers can … even place trackers or cookies on your browsers … [that] track your IP address and browsing history, which third parties can exploit."[113]

172. These data brokers will then:

> take that data and pair it with other data they've collected about you, pool it together with other data they've got on you, and then share all of it with businesses who want to market to you. They can eventually build large datasets about you with things like: "browsed gym shorts, vegan, living in Los Angeles, income between $65k-90k, traveler, and single." Then, they sort you into groups of other people like you, so they can sell those lists of like-people and generate their income.[114]

[110] Tyler Katzenberger, *LA Protests Fuel California Drive To Hide Data From Trump*, POLITICO (June 11, 2025), https://www.politico.com/news/2025/06/11/la-protests-california-hide-data-trump-00400127

[111] *Id.* at 11.

[112] *Id.* at 11.

[113] Jasdev Dhaliwal, *How Data Brokers Sell Your Identity*, MCAFEE (June 4, 2024), https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/.

[114] Paul Jarvis, *The Problem with Data Brokers: Targeted Ads and Your Privacy*, FATHOM ANALYTICS (May 10, 2022), https://usefathom.com/blog/data-brokers.

173. Thus, by collecting IP addresses and Device Metadata, data brokers can track users across the Internet, compiling various bits of information about users, building comprehensive user profiles that include an assortment of information, interests, and inferences, and offering up that information for sale to the highest bidder. The "highest bidder" is a literal term, as explained below. This is a process that Defendant facilitates and benefits from.

174. As a result of Defendant's installation of the Trackers on its Website, the information of Plaintiff and Class Members is linked to any profiles these data brokers may have about them using their IP addresses and Device Metadata (or new profiles are created for Plaintiff and Class Members).

175. These profiles are then served up to companies that want to advertise on Defendant's Website, and Defendant's users become more valuable because of having their IP addresses and Device Metadata linked to these data broker profiles. Thus, Defendant is unjustly enriched through advertising revenue by installing the tracker of the Data Broker on Plaintiff's and Class Members' browsers, thus enabling Plaintiff and Class Members to be identified and deanonymized by correlating their IP addresses and Device Metadata to comprehensive profiles. But the flipside of Defendant's installation and use of these trackers is causing the extensive proliferation and dissemination of Website users' information and exposing said users to real and significant harm.

2. Real-Time Bidding

176. Once data brokers collect Website's users' IP addresses and Device Metadata and create or link that information to comprehensive user profiles, how do these data brokers "sell" or otherwise help Defendant monetizes that information? This is where real-time bidding comes in.

177. "Real Time Bidding (RTB) is an online advertising auction that uses sensitive personal information to facilitate the process to determine which digital ad will be displayed to a user on a given website or application."[115]

178. "There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs)." An SSP, which is

[115] Sara Geoghegan, *What is Real Time Bidding?*, ELECTRONIC PRIVACY INFORMATION CENTER (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/.

at least one function of the OpenX, PubMatic, Magnite, and Sovrn Trackers, as mentioned previously, "work[s] with website or app publishers to help them participate in the RTB process." "DSPs [which is what the ADNXS Tracker is[116]] primarily work with advertisers to help them evaluate the value of user impressions and optimize the bid prices they put forth."[117] And an Advertising Exchange— which Microsoft provides[118]—"allows advertisers and publishers to use the same technological platform, services, and methods, and 'speak the same language' in order to exchange data, set prices, and ultimately serve an ad."[119]

179. In other words, SSPs provide user information to advertisers that might be interested in those users, DSPs help advertisers select which users to advertise and target, and an Advertising Exchange is the platform on which all of this happens.

180. The RTB process works as follows:

> After a user loads a website or app, an SSP will send user data to Advertising Exchanges … The user data, often referred to as "bidstream data," contains information like device identifiers, IP address, zip/postal code, GPS location, browsing history, location data, and more. After receiving the bidstream data, an Advertising Exchange will broadcast the data to several DSPs. The DSPs will then examine the broadcasted data to determine whether to make a bid on behalf of their client.
>
> Ultimately, if the DSP wins the bid, its client's advertisement will appear to the user. Since most RTB auctions are held on the server/exchange side, instead of the client/browser side, the user only actually sees the winner of the auction and would not be aware of the DSPs who bid and lost. But even the losing DSPs still benefit because they also receive and collect the user data broadcasted during the RTB auction process. This information can be added to existing dossiers DSPs have on a user.[120]

[116] MICROSOFT INVEST, https://about.ads.microsoft.com/en/solutions/technology/microsoft-invest-dsp ("Microsoft Invest is a demand-side platform built for the future of video advertising.").

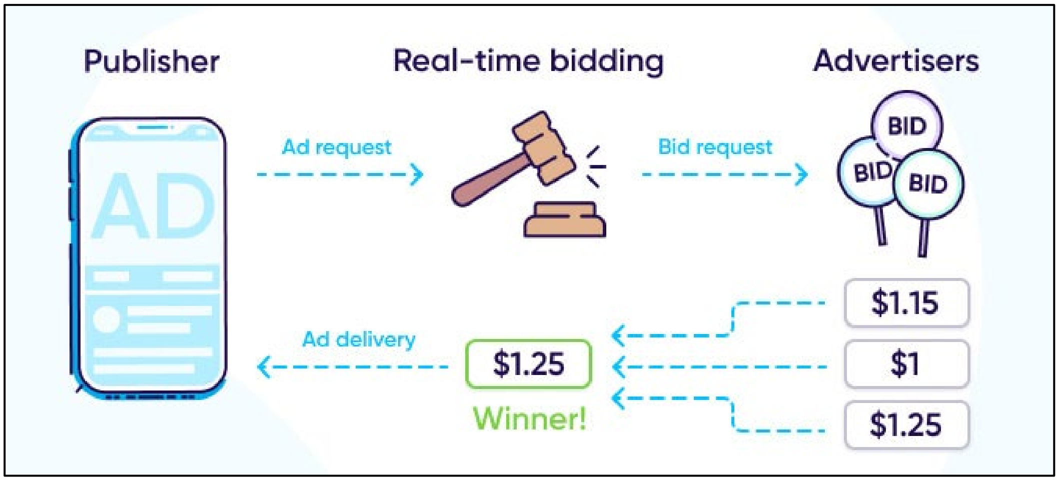
[117] Geoghegan, *supra*.

[118] Microsoft Ignite, *Microsoft Monetize - Microsoft advertising exchange inventory* (Nov. 17-21, 2025), https://learn.microsoft.com/en-us/xandr/monetize/microsoft-advertising-exchange-inventory.

[119] *Id.*

[120] Geoghegan, *supra*; *see also* REAL-TIME BIDDING, APPSFLYER, https://www.appsflyer.com/glossary/real-time-bidding/.

Figure 17:



181. Facilitating this real-time bidding process means SSPs and DSPs must have as much information as possible about Defendant's users to procure the greatest interest from advertisers and solicit the highest bids. These entities receive assistance because Defendant also installs the trackers of several data brokers (namely, OpenX, PubMatic, ID5, Tapad/Experian, and Sovrn) on its users' browsers, among others, and these trackers sync with each other to obtain complete user profiles:

> the economic incentives of an auction mean that DSP [or SSP] with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The DSP [or SSP] enlists a final actor, the data management platform (DMP) [or data brokers/identity graph providers]. DSPs send bid requests to DMPs, who enrich them by attempting to identify the user in the request and use a variety of data sources, such as those uploaded by the advertiser, collected from other sources, or bought from data brokers … thus enabling easier linkage of the data to the user's profile in the future.[121]

//

//

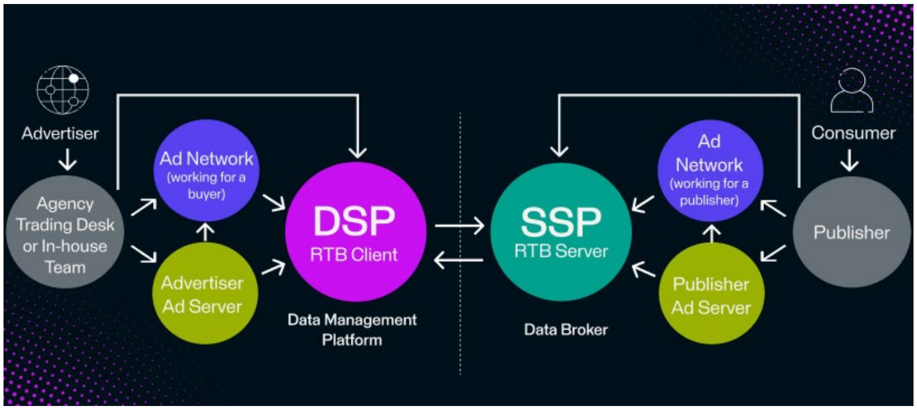
//

//

//

[121] Michael Veale & Federik Zuiderveen Borgesius, *Adtech and Real-Time Bidding under European Data Protection Law*, 23 GERMAN L. J. 226, 232-33 (2022), https://tinyurl.com/yjddt5ey; *see also* PERION, WHAT IS A SUPPLY-SIDE PLATFORM (SSP): DEFINITION AND IMPORTANCE, https://perion.com/publishers/what-is-a-supply-side-platform-ssp-definition-and-importance/.

Figure 18:



182. In other words, an SSP can solicit the highest bids for Website users by identifying and de-anonymizing those users by combining the information the SSP knows about that user with the information other data brokers know about that user. If there is a match, then the SSP will have significantly more information to provide about users, and that will solicit significantly higher bids from prospective advertisers (because the advertisers will have more information about the user to target their bids).

183. Likewise, a DSP like Microsoft can generate the highest and most targeted bids from advertisers with providing those advertisers with as much information about users as possible, which it does by syncing with PubMatic, OpenX, Magnite, ID5, Tapad/Experian, and Sovrn—who in turn, sync with other data brokers and/or are data brokers themselves.

184. Thus, Defendant's installation and use of the Third Parties' Trackers is deliberate and intended by Defendant to enrich itself through the unconsented-to sale of its users' information through the real-time bidding process.

185. As the FTC has noted, "[t]he use of real-time bidding presents potential concerns," including but not limited to:

> (a) "incentiviz[ing] invasive data-sharing" by "push[ing] publishers [*i.e.*, Defendant] to share as much end-user data as possible to get higher valuation for their ad inventory—particularly their location data and cookie cache, which can be used to ascertain a person's browsing history and behavior."
>
> (b) "send[ing] sensitive data across geographic borders."

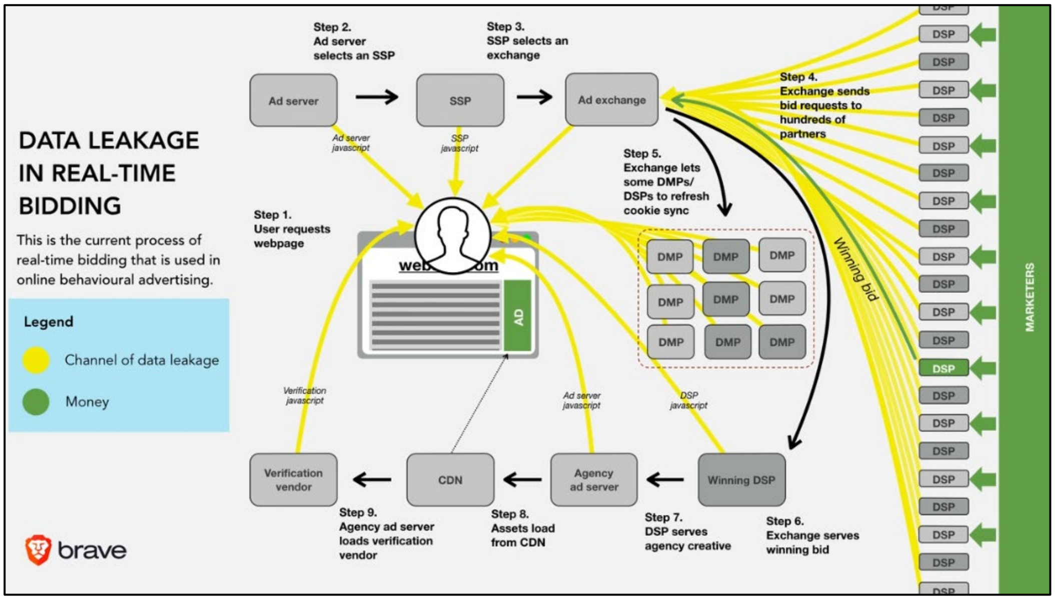
> (c) sending consumer data "to potentially dozens of bidders simultaneously, despite only one of those parties—the winning bidder actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring those other parties do not retain that data for use in unintended ways."[122]

186. Given Microsoft operates as a DSP here, the last point is particularly relevant, as it means Microsoft—through the ADNXS Tracker—collects and discloses the Website's users' information to *all prospective advertisers*, even if advertisers do not ultimately show a user an advertisement. This greatly diminishes the ability of users to control their personal information.

187. Likewise, the Electronic Privacy Information Center ("EPIC") has warned that "[c]onsumers' privacy is violated when entities disclose their information without authorization or in ways that thwart their expectations."[123]

188. For these reasons, some have characterized "real-time bidding" as "[t]he biggest data breach ever recorded" because of the sheer number of entities that receive personal information[124]:

<u>Figure 19:</u>


DATA LEAKAGE IN REAL-TIME BIDDING
This is the current process of real-time bidding that is used in online behavioural advertising.
Legend
Channel of data leakage
Money
Step 1. User requests webpage
Step 2. Ad server selects an SSP
Step 3. SSP selects an exchange
Ad server
SSP
Ad exchange
Step 4. Exchange sends bid requests to hundreds of partners
Ad server javascript
SSP javascript
Step 5. Exchange lets some DMPs/ DSPs to refresh cookie sync
web...com
AD
DMP
Winning bid
DSP
MARKETERS
Verification javascript
Ad server javascript
DSP javascript
Verification vendor
CDN
Agency ad server
Winning DSP
Step 9. Agency ad server loads verification vendor
Step 8. Assets load from CDN
Step 7. DSP serves agency creative
Step 6. Exchange serves winning bid
brave

[122] FEDERAL TRADE COMMISSION, UNPACKING REAL TIME BIDDING THROUGH FTC'S CASE ON MOBILEWALLA (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla.

[123] Geoghegan, *supra*.

[124] DR. JOHNNY RYAN, "RTB" ADTECH & GDPR, https://assortedmaterials.com/rtb-evidence/ (video).

189. All of this is in line with protecting the right to determine who does and does not get to know one's information, a harm long recognized at common law and one the CIPA was enacted to protect against. *Ribas v. Clark*, 38 Cal. 3d 355, 361 (1985) (noting the CIPA was drafted with a two-party consent requirement to protect "the right to control the nature and extent of the firsthand dissemination of [one's] statements"); *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763-64 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."); *Deivaprakash*, 798 F. Supp. 3d at 1107 (finding injury where data "collection allegedly allowed the third parties to: (1) build a profile reflecting [plaintiff's] personal information; and (2) interfere with [plaintiff's] ability to remain anonymous.").

3. Cookie Syncing

190. It should now be clear both the capabilities of the Third Parties (*i.e.*, data brokers who de-anonymize users, or companies who sync with data brokers for this purpose) and the reasons Defendant installs their Trackers on its Website (to sell to advertisers in real-time bidding with as much information about users as possible to solicit the highest bids). The final question is how do these Third Parties share information amongst each other and with others to offer the most complete user profiles up for sale? This occurs through "cookie syncing."

191. Cookie syncing is a process that "allow[s] web companies to share (synchronize) cookies and match the different IDs they assign for the same user while they browse the web."[125] This allows entities like the Third Parties to circumvent "the restriction that sites can't read each other cookies, in order to better facilitate targeting and real-time bidding."[126]

192. Cookie syncing works as follows:

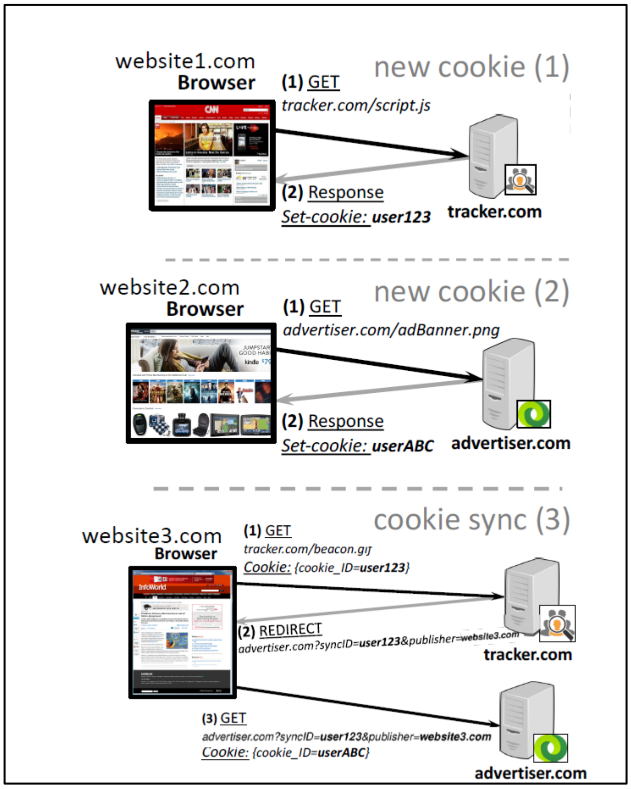
> Let us assume a user browsing several domains like website1.com and website2.com, in which there are 3rd-parties like tracker.com

[125] Panagiotis Papadopoulos et al., *Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask*, 1 WWW '19: THE WORLD WIDE WEB CONFERENCE 1432, 1432 (2019), https://dl.acm.org/doi/10.1145/3308558.3313542.

[126] Gunes Acar et al., *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*, 6B CCS'14: ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 674, 674 (2014).

> and advertiser.com, respectively. Consequently, these two 3rd-parties have the chance to set their own cookies on the user's browser, in order to re-identify the user in the future. Hence, tracker.com knows the user with the ID user123, and advertiser.com knows the same user with the ID userABC.
>
> Now let us assume that the user lands on a website (say website3.com), which includes some JavaScript code from tracker.com but not from advertiser.com. Thus, advertiser.com does not (and cannot) know which users visit website3.com. However, *as soon as the code of tracker.com is called, a GET request is issued by the browser to tracker.com (step 1), and it responds back with a REDIRECT request (step 2), instructing the user's browser to issue another GET request to its collaborator advertiser.com this time, using a specifically crafted URL (step 3)*.
>
> …
>
> When advertiser.com receives the above request along with the cookie ID userABC, it finds out that userABC visited website3.com. *To make matters worse, advertiser.com also learns that the user whom tracker.com knows as user123, and the user userABC is basically one and the same user.* Effectively, CSync enabled advertiser.com to collaborate with tracker.com, in order to: (i) find out which users visit website3.com, and (ii) *synchronize (i.e., join) two different identities (cookies) of the same user on the web.*[127]

Figure 20:



[127] Papadopoulos, *supra*, at 1433.

193. Through this process, third party trackers are not only able to resolve user identities (*e.g.*, learning that who Third Party #1 knew as "userABC" and Third Party #2 knew as "user123" are the same person), they can "track a user to a much larger number of websites," even though that "do not have any collaboration with" the third party.[128]

194. On the flip side, "CSync may re-identify web users even after they delete their cookies."[129] "[W]hen a user erases her browser state and restarts browsing, trackers usually place and sync a new set of userIDs, and eventually reconstruct a new browsing history."[130] But if a tracker can "respawn" its cookie or like to another persistent identifier (like an IP address), "then through CSync, all of them can link the user's browsing histories from before and after her state erasure. Consequently: (i) users are not able to abolish their assigned userIDs even after carefully erasing their set cookies, and (ii) trackers are enabled to link user's history across state resets."[131]

195. Thus, "syncing userIDs of a given user increases the user identifiability while browsing, thus reducing their overall anonymity on the Web."[132]

196. Cookie syncing is precisely what is happening here. When the Trackers are installed on users' of the Website's browsers, they are calling and/or syncing their cookies with other third parties on the Website. The result of this process is not only that a single user is identified as one person by these multiple third parties, but they share all the information about that user with one another (because the cookie is linked to a specific user profile). This prevents users from actually being anonymous when they visit the Website.

* * *

197. To summarize the proceeding allegations, two of the Third Parties, OpenX and PubMatic, are data brokers and identity graph providers that focus on collecting as much information about Website users as possible to create comprehensive user profiles, and sync with numerous other

[128] Papadopoulos, *supra*, at 1434.

[129] *Id.*

[130] *See id.*

[131] *Id.*

[132] *Id.* at 1441.

data brokers that do the same. The Third Parties may collect IP Addresses, Device Metadata, and unique user IDs in the first instance, but those are connected to information it gleans from other sources (*e.g.*, various data brokers) to build comprehensive profiles. Through "cookie syncing," those profiles are shared between the Third Parties and with other data brokers to form the most fulsome picture with the most attributes as possible. And those profiles are offered up for sale to interested advertisers through real-time bidding using Microsoft's ADNXS Tracker, where users will command more value, the more advertisers know about a user.

198. Thus, Defendant installs and uses the ADNXS, OpenX, and PubMatic Trackers in conjunction with those they sync with to deanonymize users, sell their information to advertisers, and enrich the value Defendant's users would otherwise command by tying the data they obtain directly from users on the Website (*e.g.*, IP addresses, Device Metadata, unique user IDs) with comprehensive user profiles.

199. Accordingly, Defendant is using the Tracker in conjunction with other parties to (i) deanonymize users, (ii) offer its users up for sale in real-time bidding, and (iii) monetize its Website by installing the Trackers and allowing the Third Parties to collect as much information about Website users as possible (without consent).

200. Thus, Defendant is unjustly enriched through its installation and use of the Trackers, which causes data to be collected by Third Parties without Plaintiff's and Class Members' consent, and that enables the Third Parties to sell Defendant's user inventory in an ad-buying system. In addition, Plaintiff and Class Members lost the ability to control their information, as their information ends up in the hands of data brokers, advertising inventory sellers, and a virtually unlimited number advertisers themselves without knowledge or consent.

201. Further, because Defendant installs the Tracker on Plaintiff's and Class Members' browsers, the Third Parties continue to track Plaintiff and Class Members wherever they go online, thus building even more comprehensive user profiles over time that are provided to the Third Parties' other clients (or further enrich Defendant here).

B. Defendant Uses The ADNXS Tracker For Targeted Advertising And Data Monetization

202. Microsoft describes its advertising services, which include the ADNXS or Microsoft Invest Tracker, as "a strategic buying platform built for the needs of today's advertisers looking to invest in upper funnel buying and drive business results."[133]

203. Microsoft collects data to help companies with their marketing; when the processing system "receives ad requests, [it] applies data to the request, receives bids, makes decisions, serves creatives, logs, auctions, etc."[134]

204. In particular:

> The Microsoft Advertising platform is a real-time bidding system and ad server. The main processing system is called the "impression bus." The impression bus receives ad requests, applies data to the request, receives bids, makes decisions, serves creatives, logs auctions, etc.
>
> Ad calls come in via our inventory supply partners: exchanges, SSPs, ad networks, and a few valued publishers.
>
> …
>
> Once we get the call, we overlay segment data from our server-side cookie store. Data is added to the cookie store either through Xandr segment pixels or by clients sending us a file of data. We also contact third-party data providers and overlay any available data.
>
> We contact all of the bidders on our platform. The ad call includes whatever user data belongs to each bidder, and information about the inventory. Bidders have a certain number of milliseconds in which to respond with a bid and the creative they want to serve.
>
> …
>
> The impression bus decides which bid wins based on the amount of the bid, and any preferences the publisher has about what they want served on their page. If the call was client-side, Microsoft Advertising serves the ad. If it was server-side, Microsoft Advertising passes the

[133] *About Microsoft Invest*, MICROSOFT IGNITE (Feb. 12, 2024), https://learn.microsoft.com/en-us/xandr/invest/about-invest.

[134] *Id.*

> bid and the location of the creative to the partner who will ultimately serve the ad.[135]

205. Microsoft Invest (*i.e.*, the ADNXS Tracker) provides "targeting, bidding algorithms, multi-currency support, and all the other features of a premium ad server."[136] To do this, Microsoft utilizes data from its cookie store. The "[d]ata is added to the cookie store either through Microsoft Advertising segment pixels or by clients sending [them] a file of data. [They] also contact third-party data providers and overlay any available data."[137]

206. As alleged above, Microsoft also integrates with the data brokers whose trackers Defendant installs on the Website. This provides Microsoft to de-anonymize and identify Website users, which it provides to advertisers so those advertisers can best target their advertisements. And, because Defendant's users have now been de-anonymized and identified, Defendant derives additional revenue from this process because advertisers will pay more to show advertisements to Defendant's users. Likewise, Defendant can effectively target users across the Internet.

207. In other words, when users visit Defendant's Website, Microsoft collects users' IP addresses and Device Metadata through its ADNXS Tracker to provide to advertisers interested in showing an advertisement to Defendant's Website users, enriching that information by integrating with other Trackers (and its own data), and ultimately enabling Defendant to monetize its Website and maximize revenue by allowing Microsoft to collect and disclose user information.

C. Defendant Uses The Pubmatic Tracker For Identity Resolution, Targeted Advertising, And Data Monetization

208. As noted above, PubMatic is a registered data broker in California that describes itself as a digital advertising platform that "exist[s] to enable content creators to run a more profitable advertising business, which in turn allows them to invest back into the multi-screen and multi-format content that consumers demand."[138]

[135] https://learn.microsoft.com/en-us/xandr/invest/about-invest

[136] *Id.*

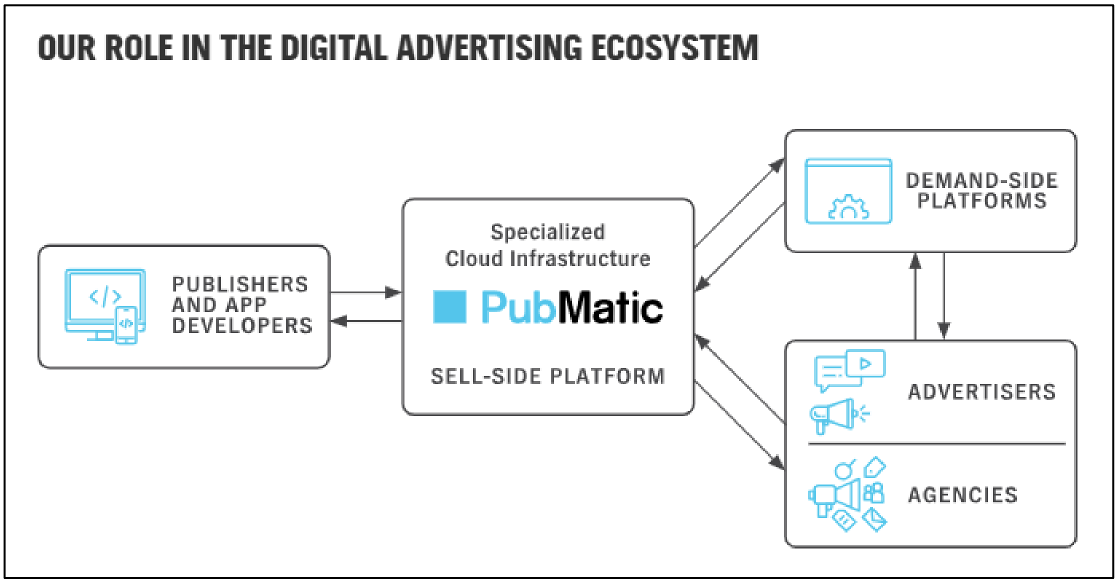
[137] *Id.*

[138] *The Supply Chain Of The Future. Delivered*, PUBMATIC, https://pubmatic.com/about-us.

209. PubMatic helps companies like Defendant monetize the data of its Website's users. As noted above, PubMatic is a "supply side platform" that helps website operators like Defendant "[m]aximize advertising revenue and control how your audiences are accessed."[139]

210. To do this, PubMatic provides a "unique, supply path optimized and addressable brand demand—from the SSP of choice for the top advertisers and agencies in the world."[140]

Figure 21:


OUR ROLE IN THE DIGITAL ADVERTISING ECOSYSTEM
PUBLISHERS AND APP DEVELOPERS
Specialized Cloud Infrastructure
PubMatic
SELL-SIDE PLATFORM
DEMAND-SIDE PLATFORMS
ADVERTISERS
AGENCIES

211. Likewise, PubMatic provides identity resolution via the "Identity Hub" service, "a leading ID management tool for publishers that leverages specialized technology infrastructure to simplify the complex alternative identifier marketplace."[141] Notably, this allows website operators like Defendant to "drive monetization in cookie-restricted environments" by "[c]onnect[ing] seamlessly with buyers to drive programmatic revenue."[142]

212. Notably, PubMatic also touts its ability to integrate with multiple other third parties—including "over 75 identity and data providers"—"leverage leading identifiers" to "help data owners

[139] PUBMATIC SSP, https://pubmatic.com/products/pubmatic-ssp-for-publishers/.

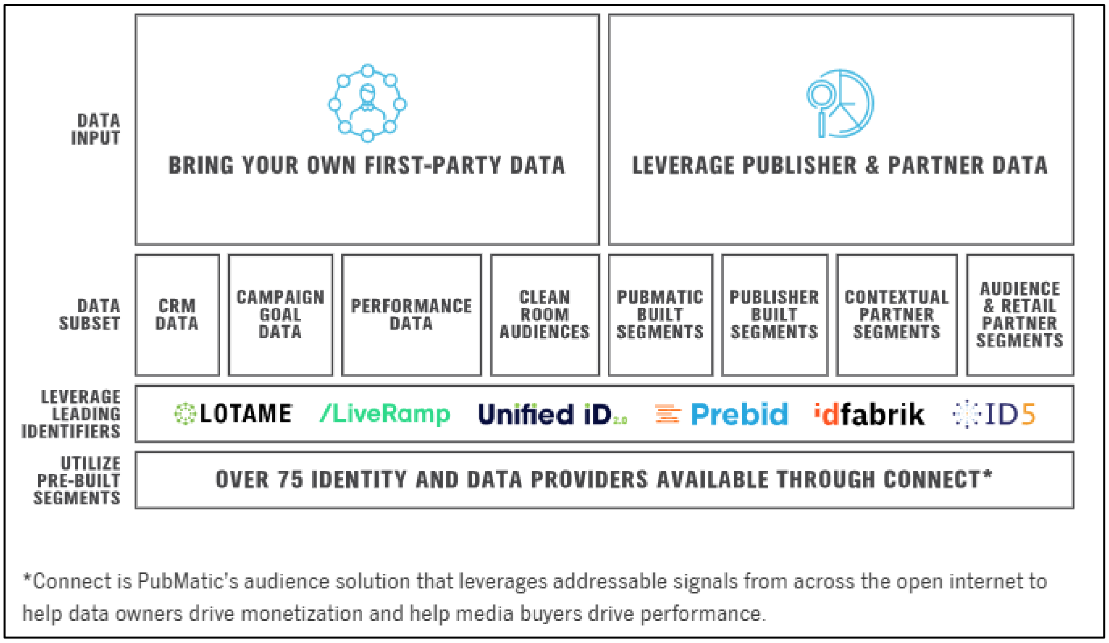
[140] *Id.*

[141] IDENTITY HUB, https://pubmatic.com/products/identity-hub/.

[142] *Id.*

[like Defendant] drive monetization and help media buyers [*i.e.*, advertisers] drive performance" including data brokers Lotame and LiveRamp[143]:

Figure 22:



DATA INPUT
BRING YOUR OWN FIRST-PARTY DATA
LEVERAGE PUBLISHER & PARTNER DATA
DATA SUBSET
CRM DATA
CAMPAIGN GOAL DATA
PERFORMANCE DATA
CLEAN ROOM AUDIENCES
PUBMATIC BUILT SEGMENTS
PUBLISHER BUILT SEGMENTS
CONTEXTUAL PARTNER SEGMENTS
AUDIENCE & RETAIL PARTNER SEGMENTS
LEVERAGE LEADING IDENTIFIERS
LOTAME
/LiveRamp
Unified iD 2.0
Prebid
idfabrik
ID5
UTILIZE PRE-BUILT SEGMENTS
OVER 75 IDENTITY AND DATA PROVIDERS AVAILABLE THROUGH CONNECT*

*Connect is PubMatic's audience solution that leverages addressable signals from across the open internet to help data owners drive monetization and help media buyers drive performance.

213. PubMatic also helps companies like Defendant "[s]mash [their] campaign KPIs [key performance indicators]" and "reach [their] target audiences more effectively."[144] One of the ways in which PubMatic accomplishes this is by selling "action packages," which are data sets—pulled together from different sources—to help advertisers target specific customers.[145]

214. In other words, PubMatic utilizes third-party data, as well as data from the publisher like Defendant where the ad is ultimately placed (*i.e.*, first-party), to determine where to place advertisers' ads and who to place them in front of.

215. By way of example, PubMatic sells a "Ramadan Auction Package" that targets consumers who observe Ramadan.[146] This package helps companies target people who have indicated interest in Ramadan Events through consumer behavior, have internet search history such

[143] PUBMATIC SSP, https://pubmatic.com/products/pubmatic-ssp-for-buyers/.

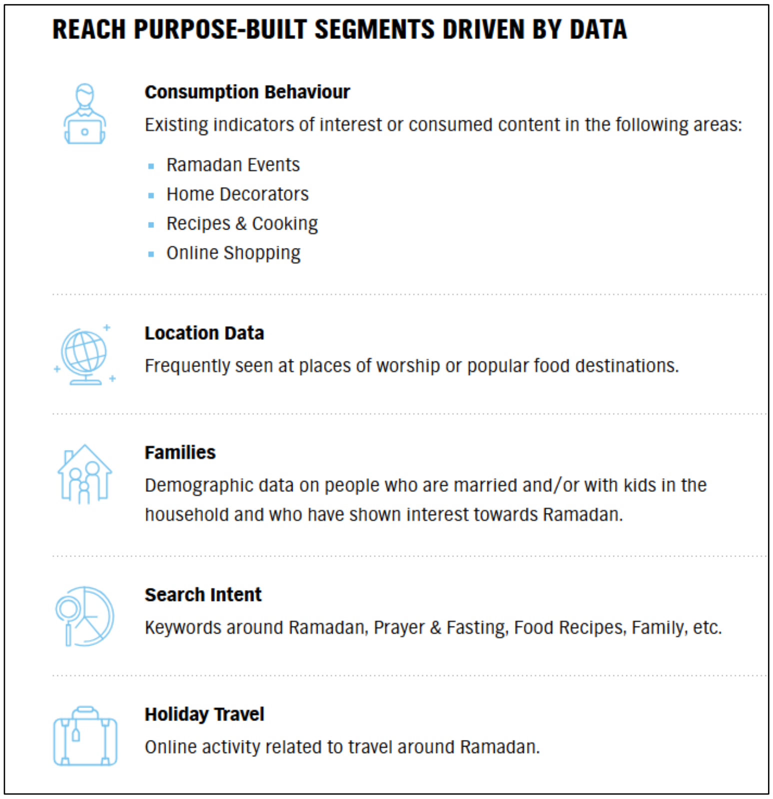
[144] CONNECT WITH PUBMATIC'S AUCTION PACKAGES, https://pubmatic.com/auction-packages.

[145] *Id.*

[146] RAMADAN AUCTION PACKAGE, https://pubmatic.com/auction-packages/us/ramadan-us/.

as "Prayer & Fasting," have location data that is "[f]requently seen at places of worship," or have "[d]emographic data" that shows they are married or live with people "who have shown interest towards Ramadan."[147]

Figure 23:



REACH PURPOSE-BUILT SEGMENTS DRIVEN BY DATA

Consumption Behaviour

Existing indicators of interest or consumed content in the following areas:

- Ramadan Events
- Home Decorators
- Recipes & Cooking
- Online Shopping

Location Data

Frequently seen at places of worship or popular food destinations.

Families

Demographic data on people who are married and/or with kids in the household and who have shown interest towards Ramadan.

Search Intent

Keywords around Ramadan, Prayer & Fasting, Food Recipes, Family, etc.

Holiday Travel

Online activity related to travel around Ramadan.

216. Thus, when users visit Defendant's Website, PubMatic records and decodes users' IP addresses, Device Metadata, and unique user ID (the KADUSERCOOKIE) through its PubMatic Tracker—as installed by Defendant—so that Defendant and PubMatic can identify users with PubMatic's suite of identity resolution services, sell Defendant's users to prospective advertisers, and ultimately reap substantial revenue through the programmatic advertising PubMatic assists with. All of this helps Defendant monetize its Website and maximize revenue by enabling PubMatic to collect as much information about Defendant's users as possible.

D. Defendant Uses The OpenX Tracker For Identity Resolution, Targeted Advertising, And Data Monetization

217. OpenX is a registered Data Broker in California.[148] It claims to be "the world's

[147] *Id.*

[148] *About Us*, OPENX, https://www.openx.com/company/.

leading independent supply-side platform (SSP) for audience, data, and identity targeting."[149] OpenX also provides an advertising exchange.

218. OpenX's "proprietary identity resolution tool, OpenAudience, uses state-of-the-art data and identity technology to allow marketers to reach their target audiences and segments — connecting [companies] to [their] desired consumers in more ways than you have ever imagined possible."[150]

219. OpenX does this by taking a company's "first-party data, or any pre-built audience segments, and seamlessly match[ing it] to [OpenX's] identity graph of more than 200 million unique people."[151]

220. In other words, OpenAudience gathers information of Defendant's Website's users, such as IP addresses and Device Metadata, compares it against their own records, and combines the two to enhance the information into a deanonymized profile of each individual website visitor.

221. OpenX can then use these individual profiles to provide marketers, such as Defendant, with curated packages that identify and target specific customers.[152]

222. OpenX splits this up into two different types of packages. The first are inventory packages that allows marketers to "[s]howcase [their] brand alongside brand-safe inventory across [OpenX's] network of trusted publishers, reaching consumers *wherever* and *whenever* they engage with their favorite content."[153] The second are data driven packages that "[e]ngage customers with packages powered by data-driven curation, and drive performance on brand-safe inventory. [Allowing companies, like Defendant to e]ffortlessly choose from pre-built packages powered by audience, contextual, attention, or sustainability data and [OpenX's] proprietary identity graph."[154]

223. This identity graph provides companies, like Defendant and the other Third Parties, access to 800 million hashed emails, 200 million hashed phone numbers, over 200 million U.S. users

[149] *Id.*

[150] *Buyers*, OPENX, https://www.openx.com/company/.

[151] *OpenAudience*, OPENX, https://www.openx.com/company/.

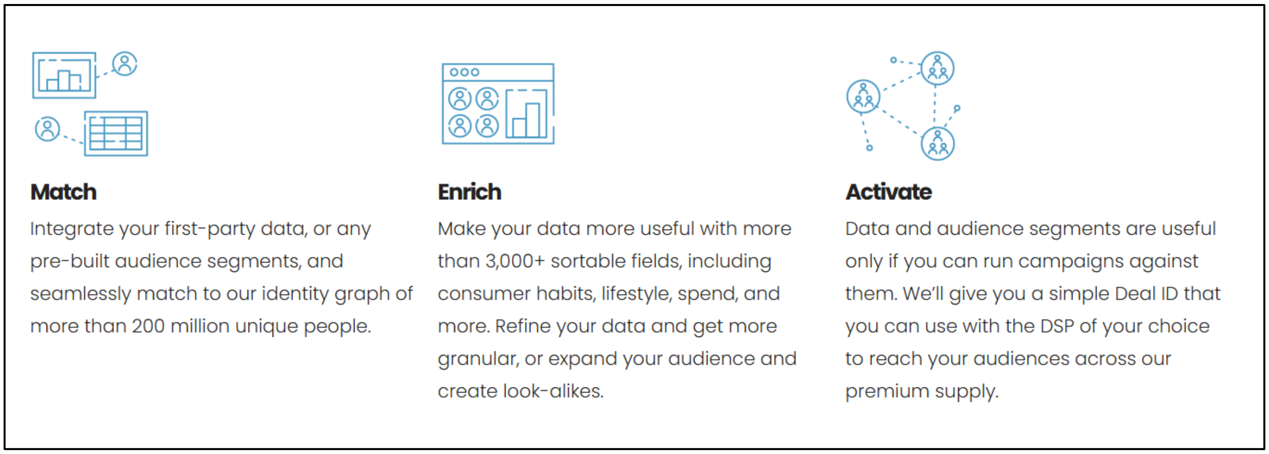
[152] *Curated Packages*, OPENX, https://www.openx.com/curated-packages/.

[153] *Id.* (emphasis added).

[154] *Id.*

instrumented for data and identity, 48 million CTV users instrumented for data and identity, over 5,000 requests per user per month, and 3,000 data attributes available for targeting.[155]

Figure 24:



Match

Integrate your first-party data, or any pre-built audience segments, and seamlessly match to our identity graph of more than 200 million unique people.

Enrich

Make your data more useful with more than 3,000+ sortable fields, including consumer habits, lifestyle, spend, and more. Refine your data and get more granular, or expand your audience and create look-alikes.

Activate

Data and audience segments are useful only if you can run campaigns against them. We'll give you a simple Deal ID that you can use with the DSP of your choice to reach your audiences across our premium supply.

224. In other words, OpenX utilizes third-party data (*i.e.*, data OpenX collects on its own), as well as data from the publisher where the ad is ultimately placed (*i.e.*, first-party, like data directly from Defendant's Website's users), to determine where to place advertisers' ads and who to place them in front of.

225. By way of example, OpenX sells a "Health Insurance Data Driven Package" that targets consumers who have viewed advertisements from health insurance advertisers.[156] This helps companies target people who have indicated an interest in specific health insurance related content.

226. To do all of this, OpenX needs to collect data that identifies a particular user. This is why OpenX collects IP addresses and Device Metadata: it allows OpenX to link one of Defendant's Website's users to any profile OpenX may have about that user, and OpenX can in turn provide that profile to interested advertisers for more targeted advertising. The IP address, Device Metadata, and OpenX cookie, also allow OpenX to track a user's Website's activity over time (*i.e.*, through repeated Website visits) and to track that user on other websites.

227. In other words, when users visit Defendant's Website, OpenX collects users' IP addresses through its OpenAudience Tracker to build comprehensive user profiles, which are used

[155] *OpenAudience*, OPENX, https://www.openx.com/company/.

[156] *Health Insurance Data Driven Package*, OPENX, https://www.openx.com/curated-packages/health-insurance/.

to identify Defendant's users, enrich Defendant's user data, and make those users more valuable to prospective advertisers by allowing advertisers to target specific users better. All of this helps Defendant further monetize its Website and maximize revenue by collecting and disclosing user information.

228. Indeed, OpenX has previously been sued by the federal government for collecting personally identifiable information from users who specifically asked not to be tracked. *See United States of America v. OpenX Technologies, Inc.*, Case No. 2:21-cv-09693-DMG-AGR (C.D. Cal.).[157]

IV. PLAINTIFF'S EXPERIENCE

229. Plaintiff regularly visits the Rotten Tomatoes Website on his desktop browser, including as recently as November 2025. The browser was set to its default settings, meaning Plaintiff was unknowingly subjected to tracking practices and served targeted advertisements because of Defendant's conduct.

230. When Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the Trackers to be installed on Plaintiff Yee's browser. *See* Figures 4, 8-9, *supra*.

231. Through their respective Trackers, the Third Parties collected Plaintiff Yee's IP address, Device Metadata, and set a cookie with a unique user ID that allowed the Third Parties to pervasively track Plaintiff across multiple Website sessions and even other websites, as well as de-anonymize Plaintiff Yee by synchronizing his user profile amongst each other and with other entities. *See* Figures 4, 6-7, 8-11, 13-15, 22-24, *supra*.

232. Defendant and the Third Parties used the information collected by the Trackers to:

(i) identity Plaintiff and either create a new profile of him or match Plaintiff to a pre-existing profile (either in Microsoft's own database or with another entity's profile)

(ii) sell Plaintiff's information to advertisers for hyper-targeted advertising based on the information collected by the Third Parties on the Website and the information contained on any profiles of Plaintiff (which are linked to Plaintiff via the information collected by the Third Parties on the Website)

[157] ADVERTISING PLATFORM OPENX WILL PAY $2 MILLION FOR COLLECTING PERSONAL INFORMATION FROM CHILDREN IN VIOLATION OF CHILDREN'S PRIVACY LAW, https://tinyurl.com/yp3f2nm5.

(iii) target Plaintiff with advertisements and serve advertisements on Plaintiff based on the information collected by the Third Parties on the Website and the information contained on any profiles of Plaintiff (which are linked to Plaintiff via the information collected by the Third Parties on the Website)

(iv) deanonymize Plaintiff and generate revenue from the sale of Plaintiff's information—both what is collected on the Website by the Parties and the profiles this information is linked to—to advertisers, thus boosting Defendant's, advertisers', and the Third Parties' revenue and the value of the Third Parties' services.

233. As an example, in the below excerpt of traffic from Plaintiff's browser on the Website, OpenX received "bid responses" from advertisers interested in showing Plaintiff an advertisement based on his information and profile. A "bid response" is "the advertiser's response to a publisher's bid request. When an advertiser decides that ad inventory offered via a bid request suits their criteria, they can respond with a bid through the RTB system. This bid response will include details about the bid as well as information on the ad campaign and the bidder."[158] In particular, OpenX received bid responses from UNICEF and Nissan to fill the same banner ad space.[159] The dimensions of the banner ad are listed as particular pixels—the values for the "h" (height) and "w" (width) parameters. These advertisers were willing to pay approximately $1.83 CPM (or "cost per mille")[160] to show Plaintiff an advertisement. That price was increased because Plaintiff was linked to non-anonymous profiles held by OpenX using the information OpenX recorded from him on the Website:

//

//

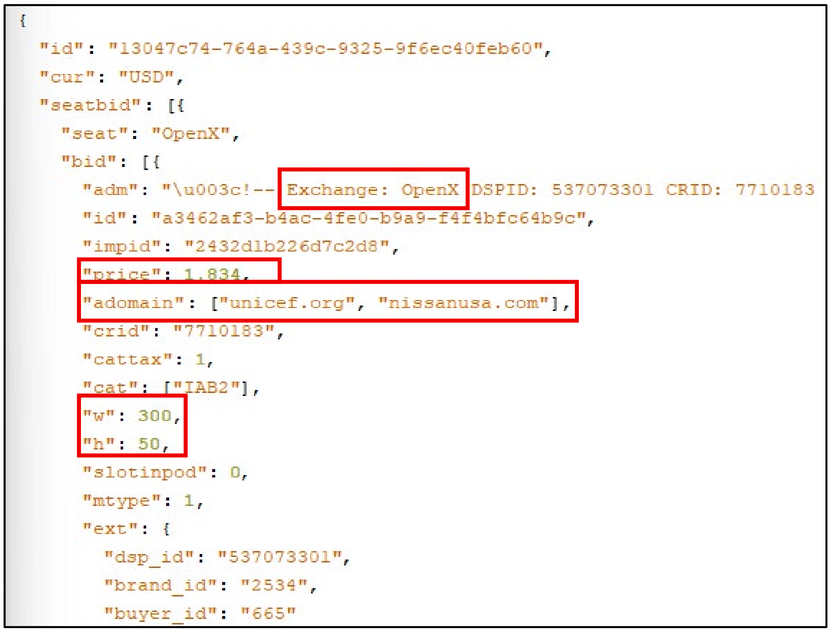
//

[158] BID RESPONSE, SMARTCLIP, https://smartclip.tv/adtech-glossary/bid-response/.

[159] "Banners are the creative rectangular ads that are shown along the top, side, or bottom of a website in hopes that it will drive traffic to the advertiser's proprietary site, generate awareness, and overall brand consideration." WHAT IS BANNER ADVERTISING?, https://advertising.amazon.com/library/guides/banner-advertising.

[160] "CPM (cost per mille) is a paid advertising option where companies pay a price for every 1,000 impressions an ad receives. An 'impression' refers to when someone sees a campaign on social media, the search engines or another marketing platform." CPM, SPROUT, https://sproutsocial.com/glossary/cpm/.

Figure 25:



```
{
  "id": "13047c74-764a-439c-9325-9f6ec40feb60",
  "cur": "USD",
  "seatbid": [{
    "seat": "OpenX",
    "bid": [{
      "adm": "\u003c!-- Exchange: OpenX DSPID: 537073301 CRID: 7710183
      "id": "a3462af3-b4ac-4fe0-b9a9-f4f4bfc64b9c",
      "impid": "2432d1b226d7c2d8",
      "price": 1.834,
      "adomain": ["unicef.org", "nissanusa.com"],
      "crid": "7710183",
      "cattax": 1,
      "cat": ["IAB2"],
      "w": 300,
      "h": 50,
      "slotinpod": 0,
      "mtype": 1,
      "ext": {
        "dsp_id": "537073301",
        "brand_id": "2534",
        "buyer_id": "665"
```

234. In other words, by installing and using the Third Parties' Trackers, Defendant and the Third Parties (i) identified Plaintiff by tying the information collected from him on the Website to profiles maintained by data brokers; and (ii) offered his data up for sale to interested advertisers through the real-time bidding process, for which Defendant received more money from advertisers based on Plaintiff's increased identifiability vis-à-vis the use of the Trackers.

235. Plaintiff did not provide his prior consent to Defendant to install or use the Trackers on his browser. Nor could Plaintiff provide prior consent to Defendant because the cookies that Defendant installed sync with Plaintiff's and the Class Members' devices the moment that they access the website. Therefore, their initial visit to the Website is automatically tracked and linked to Defendant's dossier of Plaintiff's and the Class Members' browsing activity and personal information before any consent is even possible.

236. Defendant did not obtain a court order before installing or using the Trackers.

237. Thus, Plaintiff has had his privacy invaded by Defendant's violations of CIPA § 638.51(a), and Defendant has likewise been unjustly enriched through the Third Parties' surreptitious and unconsented-to collection of Plaintiff's data.

238. Accordingly, Plaintiff has been injured by Defendant's violation of the CIPA.

CLASS ALLEGATIONS

239. Pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3), Plaintiff seeks to represent a class defined as all California residents who accessed the Website in California and had their IP addresses collected by the Trackers (the "Class").

240. The following people are excluded from the Class: (i) any Judge presiding over this action and members of her or her family; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or their parents have a controlling interest (including current and former employees, officers, or directors); (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff's counsel and Defendant's counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

241. **Numerosity:** The number of people within the Class is substantial and believed to amount to thousands, if not millions of people. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

242. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary between members of the Class, and which may be determined without reference to the individual circumstances of any Class Member, include, but are not limited to, the following:

(a) Whether Defendant violated CIPA § 638.51(a);

(b) Whether the Trackers are "pen registers" pursuant to Cal. Penal Code § 638.50(b);

(c) Whether Defendant sought or obtained prior consent—express or otherwise—from Plaintiff and the Class;

(d) Whether Defendant sought or obtained a court order for their use of the Trackers; and

(e) Whether Plaintiff and members of the Class are entitled to actual and/or statutory damages for the aforementioned violations.

243. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other members of the Class Members, visited the Website and had his IP address collected by the Trackers, which were installed and used by Defendant.

244. **Adequate Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members he seeks to represent, he has retained competent counsel experienced in prosecuting class actions, and he intends to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiff and his counsel.

245. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Class. Each individual member of the Class may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

COUNT I
Violation of the California Invasion of Privacy Act, Cal. Penal Code § 638.51(a)

246. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

247. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

248. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

249. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

250. The Trackers are "pen registers" because they are "device[s] or process[es]" that recorded or decoded the "routing, addressing, or signaling information"—the IP address, Device Metadata, and unique user IDs—from the electronic communications transmitted by Plaintiff's and Class Members' computers or smartphones. Cal. Penal Code § 638.50(b); *see also Lesh*, 767 F. Supp. 3d at 40-42.

251. Likewise, the Trackers are "pen registers" because they are "device[s] or process[es]" that are being used to ascertain the identity of visitors to Defendant's Website and is thus capturing "addressing" information. *Greenley*, 684 F. Supp. 3d at 1050 ("software that identifies consumers" is a pen register).

252. The unique IDs set by the Trackers are "addressing" information because they are used to tie a Website user to the Third Parties' databases and repositories of information about the user and ascertain the user's identity.

253. At all relevant times, Defendant installed the Third Parties' Trackers—which are pen registers—on Plaintiff's and Class Members' browsers, which allowed the Third Parties to record or decode Plaintiff's and Class Members' IP addresses and Device Metadata. The Tracker also set a unique user identifier on Plaintiff's and Class Members' browsers so the Third Parties could deanonymize Plaintiff and Class Members and track them across multiple Website sessions and multiple websites.

254. Defendant and the Third Parties used the information collected by the Trackers to:

(i) identity Plaintiff and Class Members and either create new profiles of them in Microsoft's database or match Plaintiff and Class Members to pre-existing profiles (either in the Third Parties' own databases or with another entity's profile);

(ii) sell Plaintiff's and Class Members' information to advertisers for hyper-targeted advertising based on the information collected by the Third Parties on the Website and the information contained on any profiles of Plaintiff and Class Members (which are linked to Plaintiff and Class Members via the information collected by the Third Parties on the Website);

(iii) actually target Plaintiff and Class Members with advertisements and serve advertisements on Plaintiff and Class Members based on the information collected by the Third Parties on the Website and the information contained on any profiles of Plaintiff and Class Members (which are linked to Plaintiff and Class Members via the information collected by the Third Parties on the Website); and

(iv) deanonymize Plaintiff and Class Members and generate revenue from the sale of Plaintiff's and Class Members' information—both what is collected on the Website by the Third Parties and the profiles this information is linked to—to advertisers, thus boosting Defendant's, advertisers', and the Third Parties' revenues and the value of their services.

255. When Defendant installed and used the Trackers on Plaintiff's and Class Members' browsers—and when the Third Parties collected Plaintiff's and Class Members' information—Defendant knew that Plaintiff and Class Members were in California based on their IP addresses. Thus, Defendant harmed Plaintiff and Class Members knowing they were in California and unlawfully profited off Plaintiff's and Class Members' information knowing that information came from Californians.

256. The Trackers do not collect the content of Plaintiff's and Class Members' electronic communications with the Website. *See In re Zynga Privacy Litig.* 750 F.3d 1098, 1108 (9th Cir. 2014) ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication…") (cleaned up); *Deivaprakash*, 798 F. Supp. 3d at 1106; *Fregosa v. Mashable, Inc.*, 2025 WL 2886399, at *5 (N.D. Cal. Oct. 9, 2025).

257. Plaintiff and Class Members did not provide their prior consent for Defendant's installation or use of the Trackers.

258. Defendant did not obtain a court order to install or use the Trackers.

259. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Class, naming Plaintiff as the representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order declaring that Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For statutory damages of $5,000 for each violation of CIPA § 638.51(a);

(e) For pre- and post-judgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief; and

(g) For an order awarding and the Class their reasonable attorney's fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: January 6, 2026

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Kaili C. Lynn*
Kaili C. Lynn

Kaili C. Lynn (State Bar No. 334933)
Joshua R. Wilner (State Bar No. 353949)

1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: klynn@bursor.com
jwilner@bursor.com

BURSOR & FISHER, P.A.
Philip L. Fraietta (State Bar No. 354768)
50 Main Street, Suite 475
White Plains, NY 10606
Telephone: (914) 874-0710
Facsimile: (914) 206-3656
E-mail: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Max S. Roberts (State Bar No. 363482)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-mail: mroberts@bursor.com

Attorneys for Plaintiff