BURSOR & FISHER, P.A.
Philip L. Fraietta (State Bar No. 354768)
Max S. Roberts (*Pro Hac Vice* Forthcoming)
Victoria X. Zhou (*Pro Hac Vice* Forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com
mroberts@bursor.com
vzhou@bursor.com

BURSOR & FISHER, P.A.
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: jwilner@bursor.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

KIRSTIE SEMIEN, MICHAEL SELBY, GILBERT GAW, LOGAN MITCHELL, and JANE DOE, individually and on behalf of all other persons similarly situated, Plaintiffs, v. PUBMATIC, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

TABLE OF CONTENTS

Plaintiffs Kirstie Semien, Gilbert Gaw, Michael Selby, Logan Mitchell, and Jane Doe ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against PubMatic Inc. ("PubMatic" or "Defendant"). Plaintiffs bring this action based upon personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This class action lawsuit sets forth how the business practices of PubMatic amount to constant, widespread surveillance of millions of Americans via their activity on the Internet and mobile applications. PubMatic, through its advertising and analytics products, tracks in real time and records indefinitely the personal information and specific web activity of hundreds of millions of Americans.

2. This unlawfully collected information is worth billions of dollars to Defendant because it makes up the content of PubMatic's extensive line of products, and creates individual sales of advertisements in the real-time-bidding ecosystem present on thousands of major websites.

3. Plaintiffs bring this action to enforce their constitutional rights to privacy and to seek damages under California law for the harm caused by the collection and sale of their confidential data and personal information.

THE PARTIES

4. ***Plaintiff Kirstie Semien.*** Plaintiff Kirstie Semien is a natural person and citizen of California, residing in Woodland Hills, California. Plaintiff Semien was in California when she accessed the Buzzfeed website and had her activity on that website and subsequent activity on other websites tracked by Defendant.

5. ***Plaintiff Gilbert Gaw.*** Plaintiff Gilbert Gaw is a natural person and citizen of California, residing in Redondo Beach, California. Plaintiff Gaw was in California when he accessed the Peacock website and had his activity on that website and subsequent activity on other websites tracked by Defendant.

6. ***Plaintiff Michael Selby.*** Plaintiff Michael Selby is a natural person and citizen of California, residing in Antioch, California. Plaintiff Selby was in California when he accessed the

Zillow website and had his activity on that website and subsequent activity on other websites tracked by Defendant.

7. ***Plaintiff Logan Mitchell.*** Plaintiff Logan Mitchell is a natural person and citizen of California, residing in San Diego, California. Plaintiff Mitchell was in California when he accessed the Bon Appetit website and had his activity on that website and subsequent activity on other websites tracked by Defendant.

8. ***Plaintiff Jane Doe.*** Plaintiff Jane Doe is a natural person and citizen of California, residing in Milford, California. Plaintiff Doe was in California when she made a purchase on the Mindbloom website and had her activity on that website and subsequent activity on other websites tracked by Defendants.[1]

9. ***Defendant.*** Defendant PubMatic, Inc. is a Delaware corporation with its principal place of business in Redwood City, California. PubMatic uses its proprietary technology to accomplish the widespread surveillance and unlawful sharing and sale of data alleged herein.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction 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, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from at least one Defendant.

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

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in this District.

FACTUAL ALLEGATIONS

I. DATA BROKERS AND REAL-TIME BIDDING: THE INFORMATION ECONOMY

13. To put the invasiveness of Defendant’s privacy violations into perspective, it is

[1] Because Plaintiff Doe accessed the Mindbloom website, which provides ketamine therapy, and ketamine is a Schedule III drug pursuant to the Controlled Substances Act (21 U.S.C. §§ 801, *et seq.*), Plaintiff Doe’s name has been anonymized to protect her privacy.

important to understand three concepts: data brokers, real-time bidding, and cookie syncing.

A. Data Brokers

14. While "[t]here is no single, agreed-upon definition of data brokers in United States law,"[2] 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).

15. Any entity that qualifies as a "data broker" under California law must specifically register as such (Cal. Civ. Code § 1798.99.82(a)), which PubMatic does.[3]

16. "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."[4] 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." And whereas individual data sources "may provide only a few elements about a person's activities, data brokers combine these elements to form a detailed, composite view of the consumer's life."[5]

17. For instance, as a report by NATO found, data brokers like Defendant 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.[6] Inferred data "is gleaned from observed data by modelling

[2] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy*, Duke Sanford Cyber Policy Program, at 2 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

[3] DATA BROKER REGISTRATION FOR PUBMATIC, INC., https://oag.ca.gov/data-broker/registration/186702.

[4] Sherman, *supra*, at 2.

[5] 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.

[6] Henrik Twetman & Gundars Bergmanis-Korats, *Data Brokers and Security*, at 11, NATO Strategic Communications Centre Of Excellence, (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

or profiling," meaning what consumers may be *expected* to do.[7] On top of this, "[b]rokers typically collect not only what 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."[8]

18. 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."[9] 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."[10]

19. 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."[11]

20. 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. Many industries from health insurance to life insurance to banking to e-

[7] *Id.*

[8] *Id.*

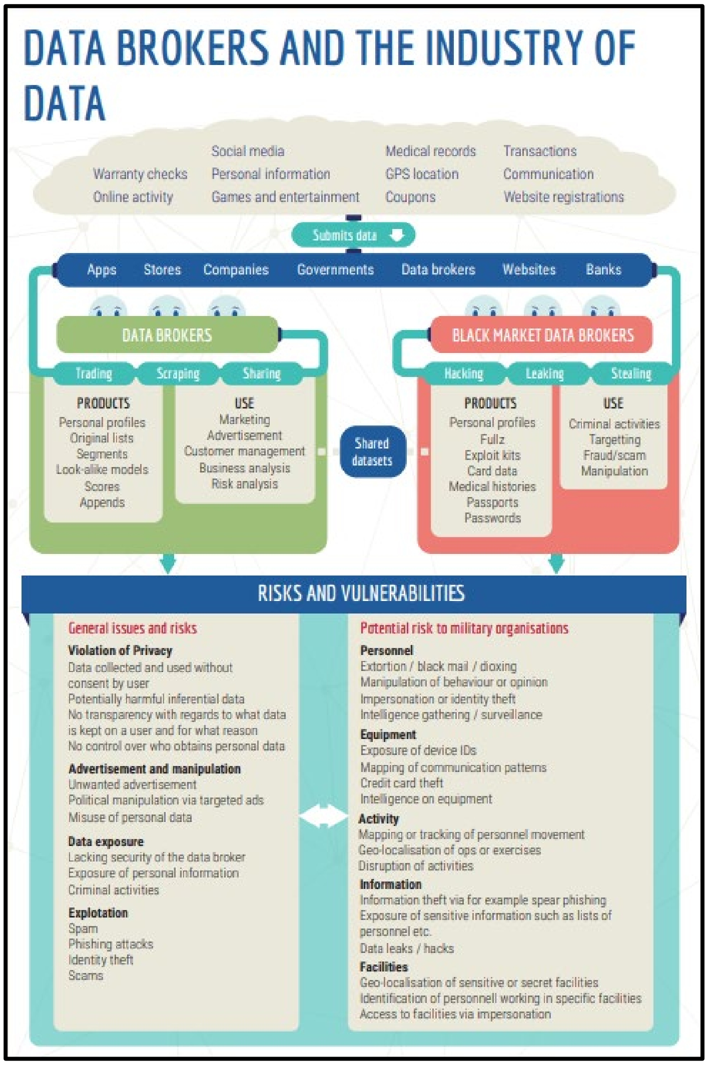
[9] Sherman, *supra*, at 1.

[10] *Id.*

[11] *Id.* at 9.

> 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.[12]

21. Similarly, as the report from NATO noted, corporate data brokers cause numerous privacy harms, including but not limited to depriving consumers 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.[13]


DATA BROKERS AND THE INDUSTRY OF DATA
Social media
Medical records
Transactions
Warranty checks
Personal information
GPS location
Communication
Online activity
Games and entertainment
Coupons
Website registrations
Submits data
Apps
Stores
Companies
Governments
Data brokers
Websites
Banks
DATA BROKERS
BLACK MARKET DATA BROKERS
Trading
Scraping
Sharing
Hacking
Leaking
Stealing
PRODUCTS
Personal profiles
Original lists
Segments
Look-alike models
Scores
Appends
USE
Marketing
Advertisement
Customer management
Business analysis
Risk analysis
Shared datasets
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

[12] *Id.*

[13] Twetman & Bergmanis-Korats, *supra*, at 8.

22. Data brokers, like Defendant, are able to compile such wide swaths of information in part by collecting users' IP addresses and other device information, which is used by data brokers like Defendant to track users across the Internet.[14] 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."[15]

23. 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.[16]

24. In short, data brokers like Defendant track consumers 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.

B. Real-Time Bidding

25. So, once data brokers like Defendant collect information from consumers and create comprehensive user profiles, how does Defendant "sell" or otherwise monetize that information? This is where real-time bidding comes in.

26. "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."[17]

[14] *Id*. at 11.

[15] Jasdev Dhaliwal, *How Data Brokers Sell Your Identity*, McAfee (Jan. 28, 2025), https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/.

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

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

27. "There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs)."[18] An SSP—which is at least one of the services Defendant provides here—"work[s] with website or app publishers to help them participate in the RTB process."[19] "DSPs primarily work with advertisers to help them evaluate the value of user impressions and optimize the bid prices they put forth."[20] And an Advertising Exchange "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 add."[21]

28. 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.

29. 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.[22]

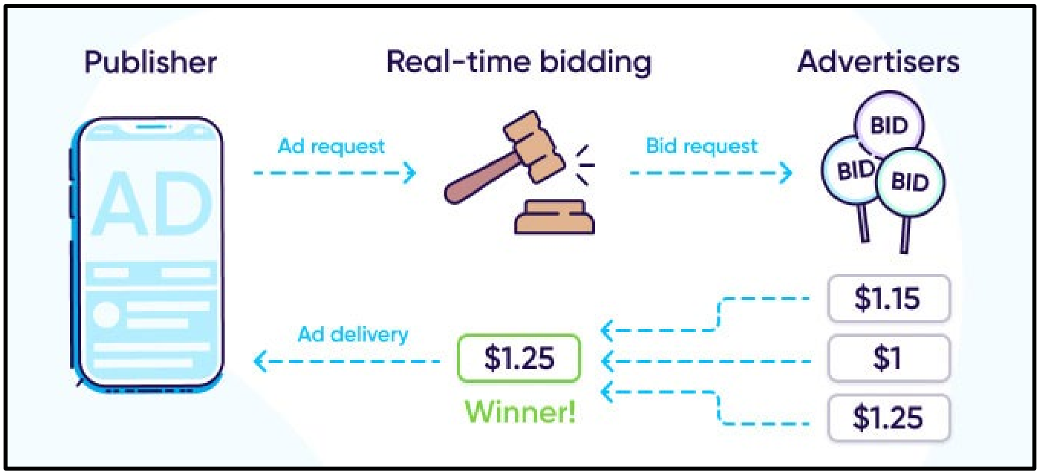
[18] *Id.*

[19] *Id.*

[20] *Id.*

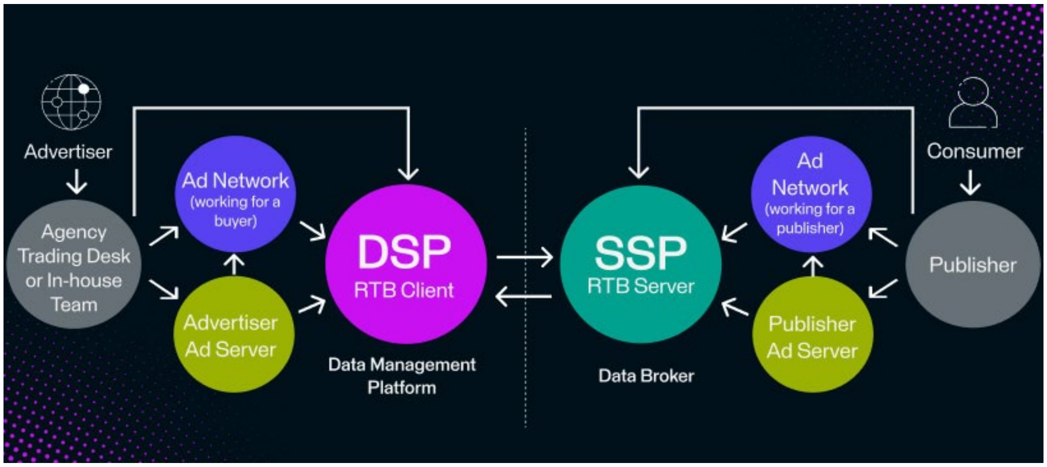
[21] *Introduction To Ad Serving*, Microsoft (Mar. 3, 2024), https://learn.microsoft.com/en-us/xandr/industry-reference/introduction-to-ad-serving.

[22] Geoghegan, *supra* note 15; *see also Real-Time Bidding*, AppsFlyer, https://www.appsflyer.com/glossary/real-time-bidding/.



30. Facilitating this real-time bidding process means SSPs and DSPs must have as much information as possible about consumers to procure the greatest interest from advertisers and obtain the highest bids for website and app operators' users. But these SSPs and DSPs receive assistance by connecting with Data Management Platforms ("DMPs") or data brokers like Defendant:

> the economic incentives of an auction mean that DSP 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 enlists a final actor, the data management platform (DMP) [or data broker, like Defendant]. 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 The DSP also wins the right to cookie sync its own cookies with those from the [Advertising Exchange], thus enabling easier linkage of the data to the user's profile in the future.[23]



[23] 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/.

31. In other words, before bidding to show a user an advertisement, a DSP will attempt to determine what other information about a user may be available. A DSP does this by connecting with DMPs, which match a consumer's information from a particular website or mobile application (*e.g.*, their IP address) with any profiles on those users Defendant may have compiled. If there is a match, then advertisers will pay more money to show users an advertisement because the advertisers have more information to base their targeting on. This naturally enriches website and app operators, as their users are now more valuable. And, a DSP is able to continue linking users on a website or mobile application through the Advertising Exchange, which enhances the DSP's ability to better identify users in the future and helps the DSP profit further as well.

32. As the Federal Trade Commission ("FTC") has noted, "[t]he use of real-time bidding presents potential concerns," including but not limited to:

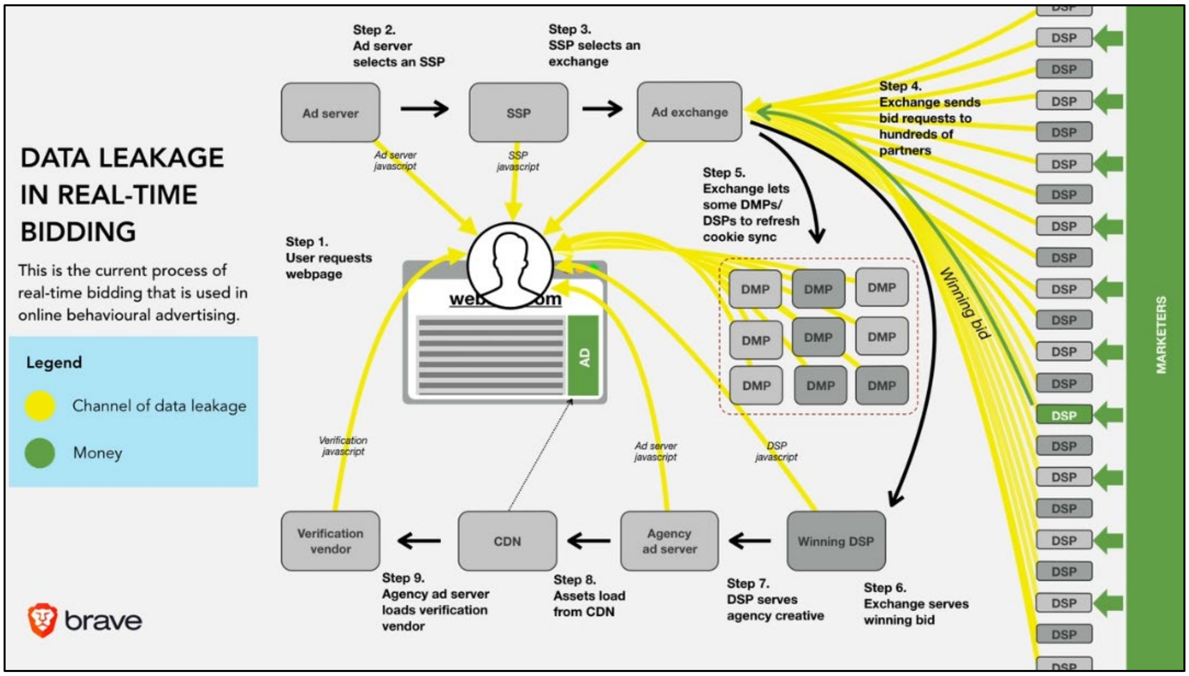
> (a) "incentiviz[ing] invasive data-sharing" by "push[ing] publishers [*i.e.*, website and app operators] to share as much end-user data as possible to get higher valuation for their ad inventory—particularly their location data and cookie cache, which can be used to ascertain a person's browsing history 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."[24]

33. The last point bears additional emphasis, as it means the data Defendant provides to DSPs to serve targeted advertisements is even provided to those entities who do not actually serve an advertisement on a consumer. This greatly diminishes the ability of users to control their personal information.

[24] Office of Technology & Division of Privacy and Identity Protection, *Unpacking Real Time Bidding through FTC's case on Mobilewalla*, Federal Trade Commission (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla.

34. 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."[25]

35. 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[26]:


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
brave
Step 1. User requests webpage
Step 2. Ad server selects an SSP
Step 3. SSP selects an exchange
Step 4. Exchange sends bid requests to hundreds of partners
Step 5. Exchange lets some DMPs/ DSPs to refresh cookie sync
Step 6. Exchange serves winning bid
Step 7. DSP serves agency creative
Step 8. Assets load from CDN
Step 9. Agency ad server loads verification vendor
Ad server
SSP
Ad exchange
Ad server javascript
SSP javascript
web...om
AD
DMP
Winning bid
DSP
MARKETERS
Verification javascript
Ad server javascript
DSP javascript
Verification vendor
CDN
Agency ad server
Winning DSP

36. 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 statutes like the CIPA were 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"); *U.S. 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.").

[25] Geoghegan, *supra* note 15.

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

C. Cookie Syncing

37. It should now be clear both the capabilities of data brokers like Defendant who de-anonymize users, and the reasons that Defendant's technology is installed on websites (to provide more information to advertisers in real-time bidding. The final question is how does Defendant share information with other services to offer the most complete user profiles up for sale? This occurs through "cookie syncing."

38. 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."[27] This allows entities like the Third Parties to circumvent "the restriction that sites can't read each other['s] cookies, in order to better facilitate targeting and real-time bidding."[28]

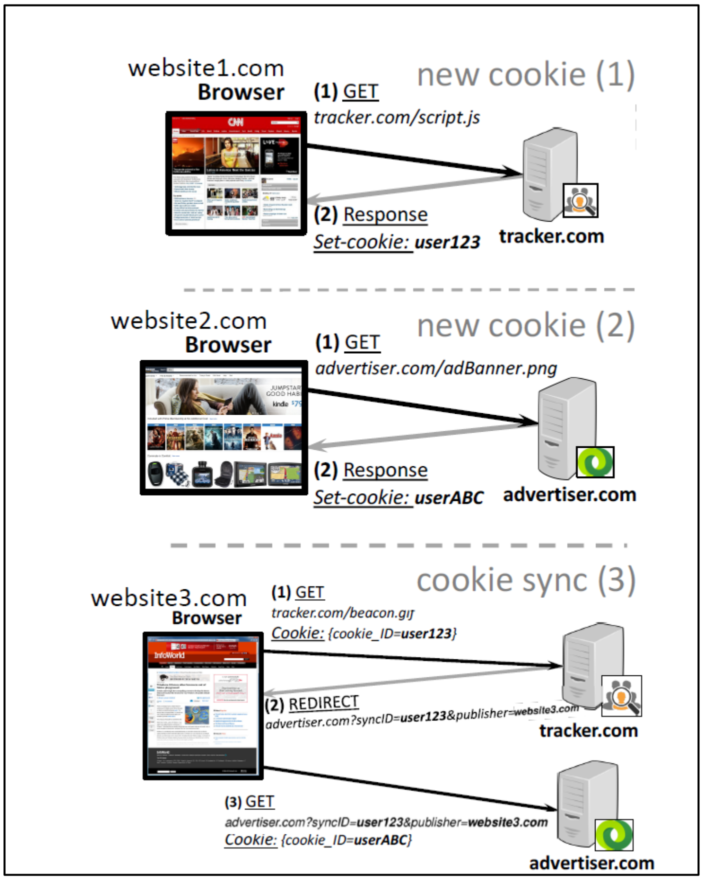
39. Cookie syncing works as follows:

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

[27] 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.

[28] 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).

> 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.*[29]



40. Through this process, third party trackers like Defendant's 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.[30]

41. On the flip side, "CSync may re-identify web users even after they delete their cookies."[31] "[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."[32] But if a tracker can "respawn" its cookie or like to another persistent identifier (like an IP address), "then through

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

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

[31] *Id.*

[32] *See id.*

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."[33]

42. Thus, "syncing userIDs of a given user increases the user identifiability while browsing, thus reducing their overall anonymity on the Web."[34]

43. Cookie syncing is precisely what is happening here. When Defendant's Pixel is installed on users' browsers, they are syncing their unique user identifiers with other third parties on the websites (*e.g.*, the Partner Pixels listed below). 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 being anonymous when they visit websites.

* * *

44. To summarize the proceeding allegations, Defendant is a data broker that focuses on collecting as much information about users as possible to create comprehensive user profiles. Through "cookie syncing," those profiles are shared by Defendant with other entities (and vice versa) to form the most fulsome picture with the most attributes as possible. And those profiles are offered up for sale to interest advertisers through real-time bidding, where users will command more value the more advertisers know about a user. Thus, Defendant enriches the value that website users would otherwise command by tying the data they obtain directly from users on websites with comprehensive user profiles in their possession or in the possession of other entities they sync with.

45. Accordingly, Defendant is using the Pixels in conjunction with website operators and other third parties to (i) de-anonymize users, (ii) offer users up for sale in real-time bidding, and (iii) allow website operators to monetize websites by installing Defendant's Pixels and allowing the Defendant to collect as much information about users as possible (without consent).

46. Of course, Defendant also benefits from this arrangement because websites and apps will want to employ Defendant's services to bring in more advertising revenue, meaning Defendant

[33] *Id.*

[34] *Id.* at 1441.

can continue to expand and grow the information they have about any consumers and add to consumers' profiles, which further perpetuates the value of Defendant's services.

47. As it stands though, Defendant is already one of the largest players in this industry. Defendant achieved this status using a variety of technologies and services, as described below.

II. AN OVERVIEW OF DEFENDANT'S ONLINE TRACKING AND ADVERTISING TECHNOLOGY

A. The PubMatic Tracker

48. PubMatic is a registered data broker in California[35] that develops and operates the PubMatic Tracker, which collects information from users' browsers and devices when they visit the websites of PubMatic's publisher clients' websites. PubMatic

49. According to PubMatic, it is "one of the world's leading scaled digital advertising platforms" and "offer[s] more transparent advertising solutions to publishers, media buyers and data owners, allowing [their clients] to harness the power and potential of the open internet to drive better business outcomes."[36]

50. PubMatic is a "supply side platform" that enables companies to sell their user inventory to advertisers, thereby earning revenue and monetizing data. To achieve this, PubMatic uses its Tracker to receive, store, and analyze information collected from website visitors, such as Plaintiffs.

51. PubMatic collects information on Internet users' activity on a wide variety of websites through the use of its Tracker, proprietary software or code it owns and develops and through partnering with other data brokers and advertisers.

52. The advertisers that PubMatic contracts with have their own pixels ("Partner Pixels"), which are integrated into the design of websites. To facilitate the identity resolution and real time bidding processes, described below, these pixels interact with and receive information from, the PubMatic Tracker when both the Partner Pixel and PubMatic Tracker are loaded onto a particular

[35] DATA BROKER REGISTRATION FOR PUBMATIC, INC., https://oag.ca.gov/data-broker/registration/186702.

[36] *The Supply Chain Of The Future. Delivered*, PUBMATIC, https://pubmatic.com/about-us (last visited Jan. 18, 2024).

website. Often, this will involve PubMatic syncing its KADUSERCOOKIE (described below) with these Partner Pixels, and having these Partner Pixels syncing their cookies with PubMatic as well.

53. Plaintiffs' testing revealed that the PubMatic Tracker interacts with, at a minimum, dozens of Partner Pixels on websites across the internet.

54. PubMatic has several methods to collect data on users. For instance, PubMatic "collects or assigns" identifiers to users' "browser or other devices to enable" their "Ad Services to determine within a reasonable level of confidence that a browser or device is the same with which [thei]r Ad Services have previously interacted."[37] These identifiers include "cookie IDs (a unique ID randomly assigned by PubMatic to a browser); unique online IDs ("UUID") created by identity providers and used by [PubMatic's] Clients; [and] mobile advertising IDs (a unique ID assigned by the mobile operating system (e.g., Apple ID for Advertising or Android Advertising ID))."[38]

55. PubMatic also collects user data through third parties such as their clients. This third party-delivered data, alongside the data PubMatic collects directly, is combined, merged and/or augmented to profile users in order to create "audience segments" that describe the hobbies and interests of users (*e.g.*, "cycling enthusiasts").[39]

56. The third-party data that PubMatic collects includes "[d]emographic or interest data" and "[p]recise geolocation information," among other types of data.[40]

57. PubMatic also discloses "cookie values to other advertising platforms" so that these platforms can match their identifiers to PubMatic's identifier.[41] This matching between PubMatic and its partners and/or clients advertising networks to provide "more relevant" advertising across their apps and on the Internet.[42]

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

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

58. All of the above information is used to identify individuals and track their activity, but wiretapping communications and collection of persistent identifiers play particular roles in the PubMatic surveillance apparatus.

1. Interception Of Communications

59. When an individual visits a website, they communicate a wide variety of information to that website. This can be as simple as their selection of an article or video the individual would like to view, but can also include highly personal information such as health status and treatment, travel plans, political affiliation, sexual orientation, and many, many more.

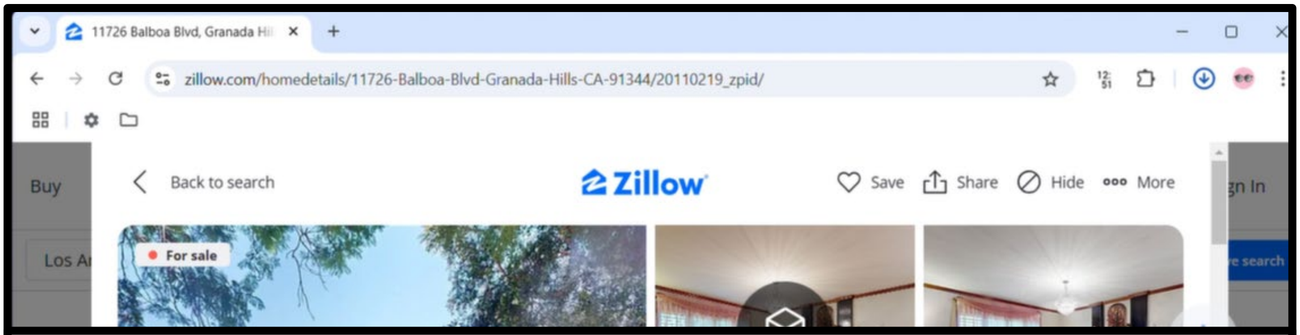
60. When the PubMatic Tracker is loaded on to a website, Defendant surreptitiously intercepts these communications. The primary way this is accomplished is through the collection of the universal resource locator ("URL") for each page of each website visited by an individual.

61. Sometimes known as a "web address," the URL is the name of the webpage as displayed in the address bar of a browser.

62. Each page on a website has its own individual URL, allowing pixels with access to the URL to see which pages of a website a particular Internet user visited.

63. All URLs identify the pages of each page of a website an internet user visited, but some—depending on the design of the website—also disclose the contents of information entered onto a webpage. These URLs are known as full-string descriptive URLs.

64. For example, when a user enters information into the Zillow website indicating the property they are interested in renting, touring, or purchasing, that information is included in the URL of the webpage and is collected by the PubMatic Tracker.


11726 Balboa Blvd, Granada Hi
zillow.com/homedetails/11726-Balboa-Blvd-Granada-Hills-CA-91344/20110219_zpid/
Buy
Los A
Back to search
Zillow
Save
Share
Hide
More
gn In
For sale
e search

```
                "page":
"https://www.zillow.com/homedetails/11726-Balboa-Blvd-Granada-Hills-CA-91344/20110219_zpid/",
                "ref": "https://www.zillow.com/",
```

65. The PubMatic Tracker collects the URL values of the pages visited by millions of internet users and, thus, intercept communications between the individuals and those websites, including sensitive information like travel information and health information.

66. As such, any pixel that intercepts the URL on this page also intercepts the content of the users' communications with Zillow about their real estate plans. This process works similarly on other websites.

67. The PubMatic Tracker collects both types of URLs and any information that can be gleaned or inferred from those URLs is added to the profiles that Defendant has for that particular user.

68. The PubMatic Tracker is configured to intercept confidential communications between internet users and websites. The intercepted information is then added to Defendant's consumer profiles and shared with bidders and advertisers as part of the real-time bidding process on thousands of websites.

2. Collection Of Persistent Identifiers

69. Another way PubMatic tracks individuals across multiple websites is through the use of persistent identifiers. As the name suggests, persistent identifiers are identifying information that follows an Internet user from one website or app to another. PubMatic uses these identifiers to confirm that a person using a particular website is the same person identified by PubMatic on another website.

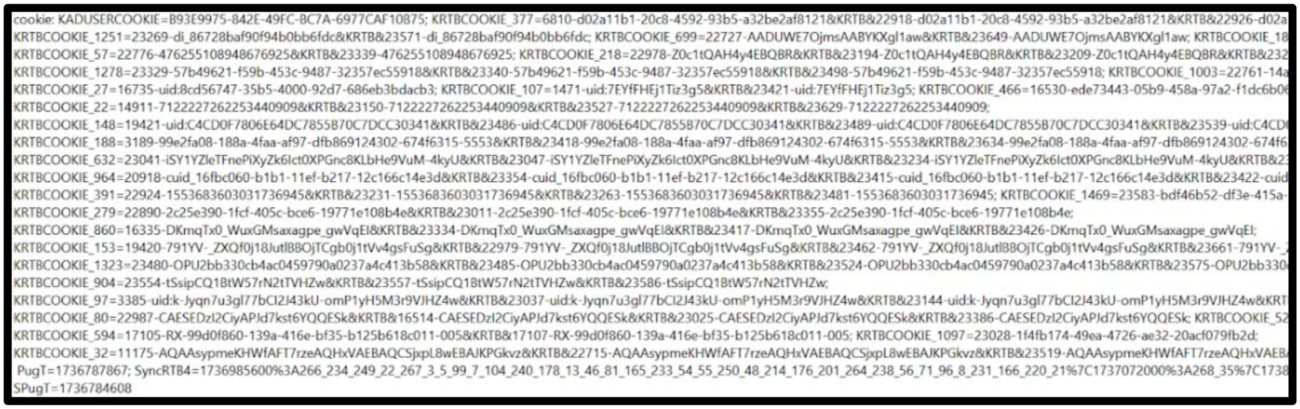
(i) <u>Unique User Identifiers</u>

70. One form of persistent identifier is a browser "cookie." "Cookies are bits of data that

are sent to and from your browser to identify you. When you open a website, your browser sends a piece of data to the web server hosting that website."[43]

71. When the PubMatic Tracker is called onto a website, it automatically downloads a cookie onto the browser of the person visiting the website. PubMatic then links a proprietary ID number to the cookie and the individual with the cookie.

72. The PubMatic Tracker also stores cookies along with the user's Device Metadata in the user's browser cache. When the user subsequently visits one of the Websites, the PubMatic Tracker locates the cookie identifiers stored on the user's browser. If the cookies are stored on the browser, the PubMatic Tracker causes the browser to send the cookies (the unique identifier, "KADUSERCOOKIE" and "KRTBCOOKIE" below) along with the user's Device Metadata to PubMatic. The KRTBCOOKIE and KADUSERCOOKIE are specifically used to "uniquely identify each browser or device from which an individual user visits our partners' websites."[44]



```
cookie: KADUSERCOOKIE=B93E9975-842E-49FC-BC7A-6977CAF10B75; KRTBCOOKIE_377=6810-d02a11b1-20c8-4592-93b5-a32be2af8121&KRTB&22918-d02a11b1-20c8-4592-93b5-a32be2af8121&KRTB&22926-d02a
KRTBCOOKIE_1251=23269-di_86728baf90f94b0bb6fdc&KRTB&23571-di_86728baf90f94b0bb6fdc; KRTBCOOKIE_699=22727-AADUWE7OjmsAABYKXgl1aw&KRTB&23649-AADUWE7OjmsAABYKXgl1aw; KRTBCOOKIE_18
KRTBCOOKIE_57=22776-476255108948676925&KRTB&23339-476255108948676925; KRTBCOOKIE_218=22978-Z0c1tQAH4y4EBQBR&KRTB&23194-Z0c1tQAH4y4EBQBR&KRTB&23209-Z0c1tQAH4y4EBQBR&KRTB&232
KRTBCOOKIE_1278=23329-57b49621-f59b-453c-9487-32357ec55918&KRTB&23340-57b49621-f59b-453c-9487-32357ec55918&KRTB&23498-57b49621-f59b-453c-9487-32357ec55918; KRTBCOOKIE_1003=22761-14a
KRTBCOOKIE_27=16735-uid:8cd56747-35b5-4000-92d7-686eb3bdacb3; KRTBCOOKIE_107=1471-uid:7EYfFHEj1Tiz3g5&KRTB&23421-uid:7EYfFHEj1Tiz3g5; KRTBCOOKIE_466=16530-ede73443-05b9-458a-97a2-f1dc6b06
KRTBCOOKIE_22=14911-7122227262253440909&KRTB&23150-7122227262253440909&KRTB&23527-7122227262253440909&KRTB&23629-7122227262253440909;
KRTBCOOKIE_148=19421-uid:C4CD0F7806E64DC7855B70C7DCC30341&KRTB&23486-uid:C4CD0F7806E64DC7855B70C7DCC30341&KRTB&23489-uid:C4CD0F7806E64DC7855B70C7DCC30341&KRTB&23539-uid:C4CD0
KRTBCOOKIE_188=3189-99e2fa08-188a-4faa-af97-dfb869124302-674f6315-5553&KRTB&23418-99e2fa08-188a-4faa-af97-dfb869124302-674f6315-5553&KRTB&23634-99e2fa08-188a-4faa-af97-dfb869124302-674f6
KRTBCOOKIE_632=23041-iSY1YZleTFnePiXyZk6Ict0XPGnc8KLbHe9VuM-4kyU&KRTB&23047-iSY1YZleTFnePiXyZk6Ict0XPGnc8KLbHe9VuM-4kyU&KRTB&23234-iSY1YZleTFnePiXyZk6Ict0XPGnc8KLbHe9VuM-4kyU&KRTB&23
KRTBCOOKIE_964=20918-cuid_16fbc060-b1b1-11ef-b217-12c166c14e3d&KRTB&23354-cuid_16fbc060-b1b1-11ef-b217-12c166c14e3d&KRTB&23415-cuid_16fbc060-b1b1-11ef-b217-12c166c14e3d&KRTB&23422-cuid
KRTBCOOKIE_391=22924-1553683603031736945&KRTB&23231-1553683603031736945&KRTB&23263-1553683603031736945&KRTB&23481-1553683603031736945; KRTBCOOKIE_1469=23583-bdf46b52-df3e-415a-
KRTBCOOKIE_279=22890-2c25e390-1fcf-405c-bce6-19771e108b4e&KRTB&23011-2c25e390-1fcf-405c-bce6-19771e108b4e&KRTB&23355-2c25e390-1fcf-405c-bce6-19771e108b4e;
KRTBCOOKIE_860=16335-DKmqTx0_WuxGMsaxagpe_gwVqEI&KRTB&23334-DKmqTx0_WuxGMsaxagpe_gwVqEI&KRTB&23417-DKmqTx0_WuxGMsaxagpe_gwVqEI&KRTB&23426-DKmqTx0_WuxGMsaxagpe_gwVqEI;
KRTBCOOKIE_153=19420-791YV-_ZXQf0j18JutlBBOjTCgb0j1tVv4gsFuSg&KRTB&22979-791YV-_ZXQf0j18JutlBBOjTCgb0j1tVv4gsFuSg&KRTB&23462-791YV-_ZXQf0j18JutlBBOjTCgb0j1tVv4gsFuSg&KRTB&23661-791YV-_
KRTBCOOKIE_1323=23480-OPU2bb330cb4ac0459790a0237a4c413b58&KRTB&23485-OPU2bb330cb4ac0459790a0237a4c413b58&KRTB&23524-OPU2bb330cb4ac0459790a0237a4c413b58&KRTB&23575-OPU2bb330
KRTBCOOKIE_904=23554-tSsipCQ1BtW57rN2tTVHZw&KRTB&23557-tSsipCQ1BtW57rN2tTVHZw&KRTB&23586-tSsipCQ1BtW57rN2tTVHZw;
KRTBCOOKIE_97=3385-uid:k-Jyqn7u3gl77bCI2J43kU-omP1yH5M3r9VJHZ4w&KRTB&23037-uid:k-Jyqn7u3gl77bCI2J43kU-omP1yH5M3r9VJHZ4w&KRTB&23144-uid:k-Jyqn7u3gl77bCI2J43kU-omP1yH5M3r9VJHZ4w&KRT
KRTBCOOKIE_80=22987-CAESEDzI2CiyAPJd7kst6YQQESk&KRTB&16514-CAESEDzI2CiyAPJd7kst6YQQESk&KRTB&23025-CAESEDzI2CiyAPJd7kst6YQQESk&KRTB&23386-CAESEDzI2CiyAPJd7kst6YQQESk; KRTBCOOKIE_52
KRTBCOOKIE_594=17105-RX-99d0f860-139a-416e-bf35-b125b618c011-005&KRTB&17107-RX-99d0f860-139a-416e-bf35-b125b618c011-005; KRTBCOOKIE_1097=23028-1f4fb174-49ea-4726-ae32-20acf079fb2d;
KRTBCOOKIE_32=11175-AQAAsypmeKHWfAFT7rzeAQHxVAEBAQCSjxpL8wEBAJKPGkvz&KRTB&22715-AQAAsypmeKHWfAFT7rzeAQHxVAEBAQCSjxpL8wEBAJKPGkvz&KRTB&23519-AQAAsypmeKHWfAFT7rzeAQHxVAEB
 PugT=1736787867; SyncRTB4=1736985600%3A266_234_249_22_267_3_5_99_7_104_240_178_13_46_81_165_233_54_55_250_48_214_176_201_264_238_56_71_96_8_231_166_220_21%7C1737072000%3A268_35%7C1738
SPugT=1736784608
```

73. **In other words, PubMatic effectively "stamps" each cookie with its own identifier to better enable it to track individuals across the Internet.**

74. Using the KADUSERCOOKIE, KRTBCOOKIE, and other cookies—including but not limited to KCCH, PUBRETARGET, KTPCACOOKIE, COKENBLD, PUBMDCID, SyncRTB2, SyncRTB3, SyncRTB4 DPSync2, DPSync3, DPSync4, USCC, DPPIX_ON,

[43] *Everything You Need To Know About Internet Cookies*, Microsoft (Apr. 25, 2023), https://www.microsoft.com/en-us/edge/learning-center/what-are-cookies?form=MA13I2.

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

SYNCUPPIX_ON, PUBUIDSYNCUPFQ, pubsyncexp and uids—as well as IP address and device identifier information, PubMatic can track and identify Website users across the Internet.

75. The complete list of cookies or trackers utilized, operated, owned or managed by PubMatic is not available to Plaintiff but is known to PubMatic.

76. This information is cross-referenced with other information collected by PubMatic to specifically identify the individual using the device and to add this web-activity information to a larger profile on the individual in order to sell their profile for targeted advertising.

(ii) <u>IP Addresses</u>

77. IP addresses are another common persistent identifier.

78. 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."[45]

79. An IP address is a unique set of numbers assigned to a device on a network, which is typically 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.[46]

80. 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

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

[46] *See, e.g.*, *What is the Internet Protocol?* CloudFlare, https://www.cloudflare.com/learning/network-layer/internet-protocol/ (last accessed Feb. 12, 2025); *What is an RFC1918 Address?* Netbeez (Jan. 22, 2020), https://netbeez.net/blog/rfc1918/.

identifying a device on the Internet or within a local network, facilitating smooth communication between devices.

81. IP addresses are not freely accessible. If an individual is not actively sending data packets out, their IP address remains private and is not broadcast to the wider internet.

82. 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.[47] Thus, "IP targeting provides a level of specificity and personalization that was never feasible through traditional media or past iterations of digital targeting."[48]

83. An IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[49] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests."[50] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[51] because "[c]ompanies can use an IP address … to personally identify individuals."[52]

84. In fact, an 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 [them] an inside look into where they are, where they have been, and what kinds of products or

[47] *IP Location Lookup*, IPLOCATION.IO, https://iplocation.io/ (last accessed Feb. 14, 2025).

[48] IP TARGETING 101: SMART DISPLAY ADVERTISING, https://www.dbswebsite.com/blog/ip-targeting-101-smart-display-advertising/ (last accessed Mar. 28, 2025).

[49] *Location-based Targeting That Puts You in Control*, choozle, https://choozle.com/geotargeting-strategies/ (last accessed Feb. 12, 2025).

[50] Herbert Williams, *The Benefits of IP Adress Targeting for Local Businesses*, Linkedin (Nov. 29, 2023), https://tinyurl.com/4uk2p7k9.

[51] *IP Targeting: Understanding This Essential Marketing Tool,* ACCUDATA (as accessed Apr.1, 2023), https://web.archive.org/web/20230401042804/https://www.accudata.com/blog/ip-targeting/.

[52] 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/.

services will appeal to their needs."[53] 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.[54]

85. "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."[55]

86. "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."[56]

87. In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's IP address because it "can be more cost-effective than other forms of advertising."[57] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[58]

88. Further, "IP address targeting can help businesses to improve their overall marketing strategy."[59] "By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts."[60]

89. Putting IP addresses in the hands of a data broker like PubMatic is particularly invasive, as the NATO report noted:

[53] *Geomarketing Strategies & Tips: The Essential Guide*, Deep Sync (Jan. 3, 2025), https://deepsync.com/geomarketing/.

[54] *See, e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI , https://www.geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns (last accessed Feb. 12, 2025).

[55] *IP Targeting*, Savant DSP, https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB (last accessed Feb. 12, 2025).

[56] *Id.*

[57] Williams, *supra*.

[58] *Id.*

[59] *Id.*

[60] *Id.*

> [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.[61]

90. 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."[62]

(iii) <u>Mobile Identifiers</u>

91. PubMatic employs similar methods to track individuals using mobile apps on Android and iOS devices.

92. PubMatic owns and operates the OpenWrap "software development kit" (SDKs), a piece of code that works independently or with PubMatic's Analytics "application programming interfaces" (Analytics APIs) and is loaded into mobile apps in order to track users' activity on those apps.[63]

93. PubMatic's OpenWrap SDK connects mobile applications that use the SDK to "third-party demand" for advertising. The OpenWrap SDK "solution enables a mobile application to access demand through RTB, PMP and Header Bidding," meaning it facilitates the ad-buying process for parties that are buying and selling ad space within mobile applications.[64]

[61] Twetman & Bergmanis-Korats, *supra*, at 11.

[62] 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.

[63] *SDK vs. API: What's the difference?* IBM (July 13, 2021), https://www.ibm.com/blog/sdk-vs-api/ ("SDK" stands for software development kit and "is a set of software-building tools for a specific program," while "API" stands for application programming interface). Plaintiff will refer to both collectively as the "OpenWrap SDK" to avoid any confusion.

[64] PubMatic Product Descriptions, https://pubmatic.com/legal/program-descriptions/

94. An SDK is a "set of tools for developers that offers building blocks for the creation of an application instead of developers starting from scratch … For example, Google Analytics provides an SDK that gives insight into user behavior, engagement, and cross-network attribution."[65]

95. An API "acts as an intermediary layer that processes data transfer between systems, letting companies open their application data and functionality to external third-party developers [and] business partners."[66] An API can "work[] as a standalone solution or included within an SDK … [A]n SDK often contains at least one API."[67] APIs "enable[] companies to open up their applications' [or websites'] data and functionality to external third-party developers, business partners, and internal departments within their companies."[68]

96. Similar to the pixels on web browsers, Defendant's OpenWrap SDK is called by other SDKs when a user accesses a particular app.

97. The OpenWrap SDK tracks the types of user information Defendant obtains through the PubMatic Tracker, including but not limited to users': location information, email addresses, device and advertising identifiers, and usage of the particular app being accessed.

98. In addition to its own ID tracking, PubMatic collects advertising identifiers that are designed to track the app activity of individual users across different apps. Two of the most prominent are AAIDs (for Android devices) and IDFAs (for iOS devices) (collectively, "Mobile Advertising IDs" or "MAIDs").

99. An AAID is a unique string of numbers that attaches to a device. As the name implies, an AAID is sent to advertisers and other third parties so they can track user activity across multiple

[65] *API vs. SDK: The Difference Explained (with Examples)*, stream, https://getstream.io/glossary/api-vs-sdk/ (last accessed Feb. 13, 2025).

[66] Michael Goodwin, *What is an API (application programming interface)?* IBM, Apr. 9, 2024, https://www.ibm.com/topics/api.

[67] IBM, *supra* note 52.

[68] *Application Programming Interface*, sdxcentral, https://www.sdxcentral.com/resources/glossary/application-programmatic-interface-api/ (last accessed Feb. 13, 2025).

mobile applications.[69] So, for example, if a third party collects AAIDs from two separate mobile applications, it can track, cross-correlate, and aggregate a user's activity on both apps.

100. Although technically resettable, an AAID is a persistent identifier because average users are not aware of AAIDs and, correspondingly, virtually no one resets that identifier. The fact that the use and disclosure of AAIDs is so ubiquitous evidences an understanding on the part of Defendant, and others like Google in the field that AAIDs are almost never manually reset by users (or else an AAID would be of no use to advertisers). Byron Tau, *Means of Control: How the Hidden Alliance of Tech and Governments is Creating a New American Surveillance State*, at 175 (2024) ("Like me, most people had no idea about the 'Limit Ad Tracking' menu on their iPhones or the AAID that Google had given even Android devices. Many still don't."); *see also Louth v. NFL Enterprises LLC*, 2022 WL 4130866, at *3 (D.R.I. Sept. 12, 2022) ("While AAID are resettable by users, the plaintiff plausibly alleges that AAID is a persistent identifier because virtually no one knows about AAIDs and, correspondingly, virtually no one resets their AAID.") (cleaned up).

101. Using publicly available resources, an AAID can track a user's movements, habits, and activity on mobile applications.[70] Put together, the AAID serves as "the passport for aggregating all of the data about a user in one place."[71]

102. Because an AAID creates a record of user activity, this data can create inferences about an individual, like a person's political or religious affiliations, sexuality, or general reading and viewing preferences. These inferences, combined with publicly available tools, make AAIDs an identifier that sufficiently permits an ordinary person to identify a specific individual.

103. Similarly, an "Identifier for Advertisers, or IDFA for short, is a unique, random identifier (device ID) that Apple assigns to every iOS device. An IDFA would be the equivalent of

[69] *Advertising ID*, Google, https://support.google.com/googleplay/android-developer/answer/6048248 (last accessed Feb. 13, 2025).

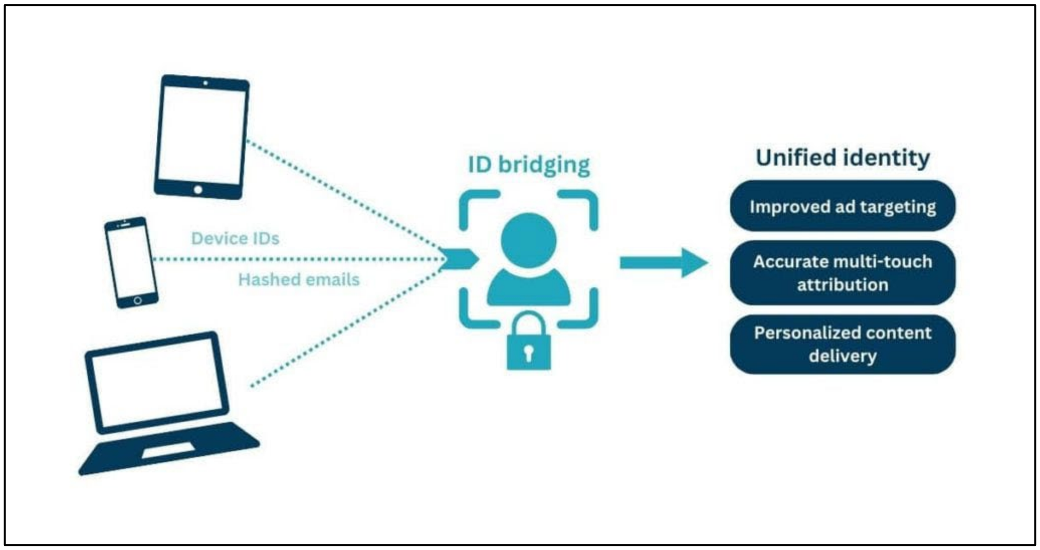
[70] Thomas Tamblyn, *You Can Effectively Track Anyone, Anywhere Just By the Adverts They Receive*, HuffPost, Oct. 19, 2017, https://www.huffingtonpost.co.uk/entry/using-just-1000-worth-of-mobile-adverts-you-can-effectively-track-anyone_uk_59e87ccbe4b0d0e4fe6d6be5.

[71] *Trend Report: Apps Oversharing Your Advertising ID*, International Digital Accountability Council, https://digitalwatchdog.org/trend-report-apps-oversharing-your-advertising-id/ (last accessed Feb. 13, 2025).

a web cookie, in the sense that it enables advertisers to monitor users' engagement with their ads, and keep track of their post-install activity."[72]

104. PubMatic's collection of IDFAs allows PubMatic to track iOS users' activity across the various apps they use. Like the AAID, this data can create inferences about an individual, such as a person's political or religious affiliations, sexuality, or general reading and viewing preferences. These inferences, combined with publicly available tools, sufficiently permit even an ordinary person to identify a specific individual with the IDFA.

105. Regardless of whether these IDs are supposed to be anonymous, MAIDs are often combined with other identifiers to identify users in what is known as ID Bridging. "ID Bridging" is the process of "piecing together different bits of information about" a user "to confidently infer that it is the same individual accessing a publisher's site or sites from various devices or browsers."[73] That is, users can be identified and tracked by "bridging" (or linking) their MAIDs to other sources, such as e-mail addresses, geolocation, or phone numbers.



[72] *Identifier for Advertisers (IDFA)*, Apps Flyer, https://www.appsflyer.com/glossary/idfa/ (last accessed Feb. 13, 2025).

[73] Kayleigh Barber, *WTF is the difference between ID bridging and ID spoofing?* Digiday, July 9, 2024, https://digiday.com/media/wtf-is-the-difference-between-id-bridging-and-id-spoofing/.

106. ID Bridging "has long been the foundation of the programmatic advertising,"[74] which is another name for the real-time bidding process alleged above. It entails a "unique identifier [] assigned to individual devices," personal information like geolocation and e-mail address, and "cross-platform linkage."[75]

107. ID Bridging is a money-making machine for advertisers and app developers. On the advertiser side, ID Bridging "increase the chances of an ad buying platform finding their inventory to be addressable and, therefore, maximizes their 'ad yields.'" And on the app developer side, "publishers can boost revenue from direct-sold campaigns by offering advertisers access to more defined and valuable audiences."[76]

108. In other words, advertisers will be able to find users that are more directly and likely interested in what is being sold by having access to significantly more information. And app users' information will be more valuable (and therefore, bring in more money to app developers) because it is combined with a plethora of other information from various sources.

109. Many companies (*e.g.*, data brokers, identity graph providers), publicly advertise their ability to conduct such bridging. Yet, while those within the ID Bridging industry describe it as privacy-protective, it is anything but. As courts have noted, the "ability to amass vast amounts of personal data for the purpose of identifying individuals and aggregating their many identifiers" creates "dossiers which can be used to further invade [users] privacy by allowing third parties to learn intimate details of [users'] lives, and target them for advertising, political, and other purposes, ultimately harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them." *Katz-Lacabe v. Oracle Am., Inc*. 688 F. Supp. 3d 928, 940 (N.D. Cal. 2023) (cleaned up).

[74] Matt Keiser, *How Can ID Bridging – The Foundation of Our Space – Suddenly Be a Bad Thing?* Ad Exchanger (July 23, 2024), https://www.adexchanger.com/data-driven-thinking/how-can-id-bridging-the-foundation-of-our-space-suddenly-be-a-bad-thing/.

[75] Anete Jodzevica, *ID Bridging: The Privacy-First Future of Audience Targeting*, Setupad (Nov. 15, 2024) https://setupad.com/blog/id-bridging/.

[76] Bennett Crumbling, *What is 'ID Bridging' and how publishers use it to grow direct and programmatic revenue?* Optable (Aug. 22, 2024), https://www.optable.co/blog/what-is-id-bridging.

110. In February 2019, Oracle published a paper entitled, "Google's Shadow Profile: A Dossier of Consumers Online and Real World Life," part of which provides as accurate a description of Google's services (and Oracle's, ironically) as Defendant's:

> a consumer's "shadow profile" [is a] massive, largely hidden dataset[] of online and offline activities. This information is collected through an extensive web of … services, which is difficult, if not impossible to avoid. It is largely collected invisibly and without consumer consent. Processed by algorithms and artificial intelligence, this data reveals an intimate picture of a specific consumer's movements, socio-economics, demographics, "likes", activities and more. It may or may not be associated with a specific users' name, but the specificity of this information defines the individual in such detail that a name is unnecessary.[77]

111. In other words, ID Bridging is dangerous because of the sheer expanse of information being compiled by companies like Defendant's without the knowledge or consent of users, all of which is being done for pecuniary gain.

3. User ID Mapping and Identity Resolution

112. PubMatic offers tools so that its clients can identify the users they track. PubMatic provides its clients with technology, called Identity Hub, that allows them to simplify and combine user ID information so that ad buyers can "recognize a publisher's audience and bid more on its inventory through multiple IDs supported for each ad impression."[78]

113. PubMatic used its PubMatic Tracker and Identity Hub software to "manage multiple IDs," allowing its customers to better recognize users' advertising IDs across multiple "ID solutions."[79] Identity Hub allows PubMatic's clients to standardize, if not deanonymize, user information in order to: (1) create a more thorough profile of users' identity across multiple platforms; and (2) further understand users' habits and behavior in order to serve targeted advertisements.

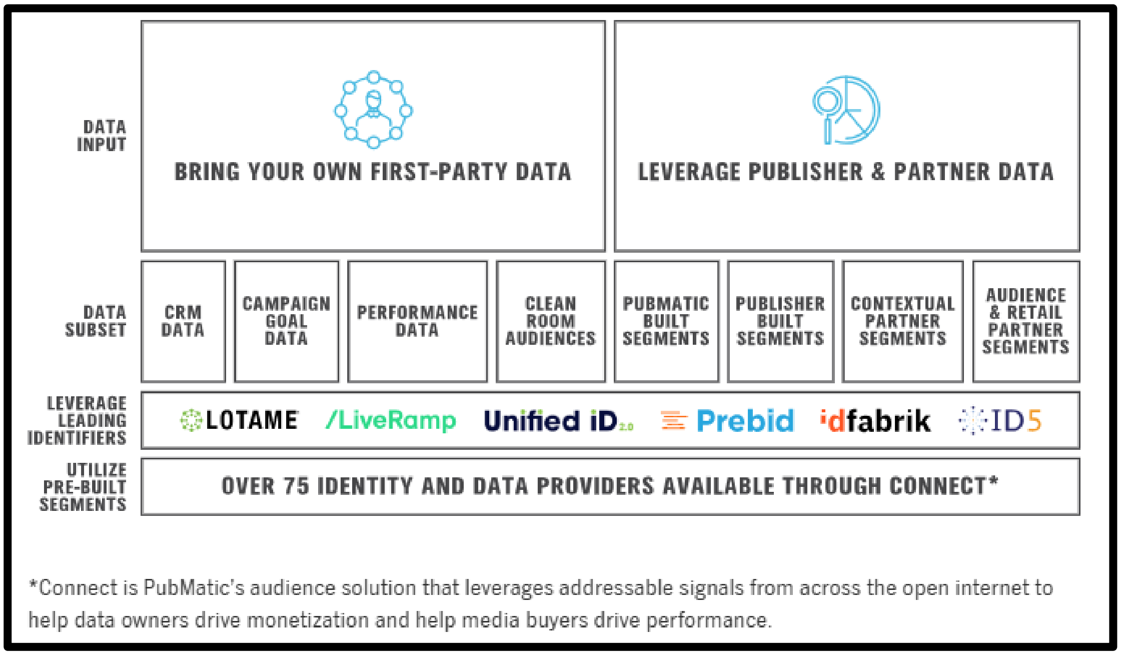
[77] *Google's Shadow Profile: A Dossier of Consumers Online and Real World Life*, Oracle, at 1 (Feb. 2019), https://tinyurl.com/2mtuh7vf.

[78] *PubMatic Launches Identity Hub To Boost Publisher Ad Revenue*, PubMatic, https://pubmatic.com/news/pubmatic-launches-identity-hub-boost-publisher-ad-revenue/

[79] *Identity Management. Delivered.*, PubMatic, https://pubmatic.com/identity-hub-acquisition-marketing-paid-search-04-2022/#tab_1

114. In plain language, identity resolution is another way to monetize PubMatic's tracking, where it assigns an ID number to an individual so that the individual is attached to a record of their web and app activity for the purpose of targeted advertising.

115. PubMatic touts its ability to integrate with multiple other third parties—including "over 75 identity and data providers"—"leverage leading identifiers" to "help data owners [like Defendant] drive monetization and help media buyers [*i.e.*, advertisers] drive performance."[80]



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.

116. Once sufficient data has been collected on an individual, Defendant monetizes the individual's data in a number of ways. One way is to provide individuals' identities and web browsing information to the companies operating the Partner Pixels to assist with those companies' collection of internet users' data.

117. This process happens when both the PubMatic Tracker and a Partner Pixel are loaded onto a website. The Partner Pixel "calls" the PubMatic Tracker and the PubMatic responds with a request that shares the individual's PubMatic ID and associated information, including the identifiers described above, with that Partner Pixel.

118. This process happens multiple times on each website, with many tracking pixels and potential advertisers gaining access to an individual's information for bidding and targeted

[80] *Id.*

advertising, enriching Defendant, the other technology companies involved, and the host websites alike while trampling consumer privacy in the process. Transmissions of this type are happening across all of the websites and apps where the PubMatic tracker is loaded.

119. With respect to the delivery of targeted advertisements on websites, Defendant's ID syncing makes the entire real-time-bidding process possible by identifying the individual visiting the site and providing information about their web activity and interests. This creates the basis for hyper-targeted advertising related to that activity and those interests to be served. This ultimately benefits the website or app operator, as it makes their userbase more valuable because said users have been further identified and linked to other activity via PubMatic's Tracker.

120. For these processes to happen, Defendant must necessarily share the information it collects on individual internet users with its partners.

121. The identity resolution service aids in the wiretapping and surveillance conducted by the Pixel Partners.

122. As part of their investigation, Plaintiffs' counsel conducted testing on several websites to provide a sample of the widespread tracking and wiretapping of, and targeted advertising to, millions of Americans by PubMatic. For each of the websites tested, there are hundreds or thousands of others where the same or similar information is collected. *See* Factual Allegations § III, *infra*.

123. Specifically, Plaintiffs' counsel found that each website and/or app had Partner Pixels loaded onto it, which in turn communicated with the PubMatic Tracker to better enable their advertising. Each Partner Pixel would itself intercept users' communications with the website or app. The PubMatic Tracker would then assign a PubMatic ID to the user's activity on the website or app, which, among other things, (i) allowed for the user to be identified; (ii) link the user to information from across other websites and apps; and (iii) benefit the websites, apps, and Partner Pixels by making that user more valuable to advertisers because the user could be better targeted with relevant ads due to the extensive information Defendant collected and provided to the Partner Pixels.

B. PubMatic's Services

124. In addition to the PubMatic Tracker, PubMatic offers other products and services to its clients to facilitate the advertising process. PubMatic's products "offer more transparent advertising solutions to publishers, media buyers and data owners, allowing them to harness the power and potential of the open internet to drive better business outcomes."[81] In other words, PubMatic offers a portfolio of products that provide its clients the technology to buy and sell digital advertising space, data management, and analytics tools. PubMatic's technology offerings include real-time bidding, a proprietary private marketplace, a wrapper solution (the Openwrap SDK), OpenWrap OTT (a service for managing over-the-top media content on various smart devices with built in advertising, like smart televisions), Identity Hub, and its Analytics API.[82] PubMatic is a supply-side platform.

125. PubMatic partners with third-party providers or partners such as ABC, Microsoft, WebMD, Verizon, Chegg, eBay, Forbes, Zillow, Univision, and the New York Times, among others, all of whom receive PubMatic platform data and other consumer information (however, the extent of this data is unknown). As a result, PubMatic shares information about consumers with over thirty thousand partners.[83]

126. PubMatic's partners receive varying amounts of data depending on their relationship with PubMatic. PubMatic's publisher partners receive browser and device information, behavioral information, ad interaction, geolocation, audience segments and ID sync data. PubMatic's media buyer partners receive browser and device information, behavioral information, ad interaction, partner provided information, geolocation, audience segments, ID sync data, and business administration information. PubMatic's attribution and analytics partners receive browser and device information; behavioral information; ad interaction; partner provided information; geolocation;

[81] *The Supply Chain of the Future. Built For You.*, PubMatic, https://pubmatic.com/about-us/ (last accessed Mar. 25, 2025).

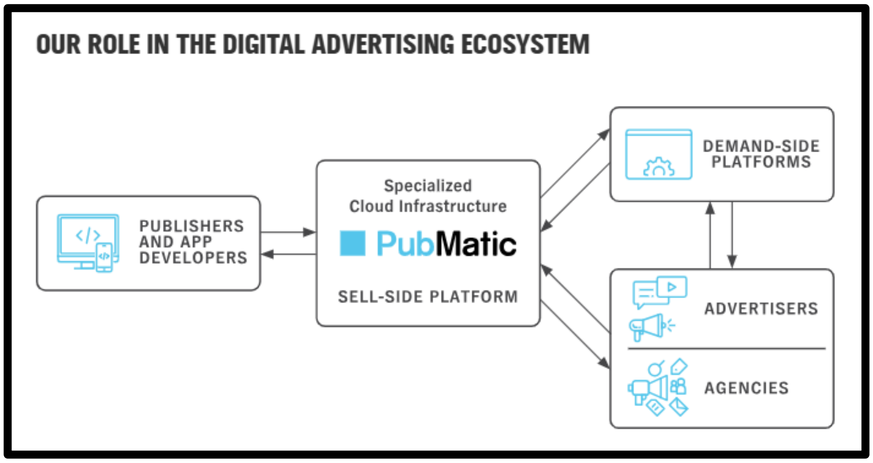
[82] PubMatic Product Descriptions, https://pubmatic.com/legal/program-descriptions/

[83] Technology Profile, PubMatic, *6sense*, https://6sense.com/tech/supply-side-platform-ssp/pubmatic-market-share

audience segments and ID sync data.[84]

133. PubMatic helps these companies monetize the data of website users. As noted above, PubMatic is a "supply side platform" that helps website operators and Partner Pixels "[m]aximize advertising revenue and control how your audiences are accessed."[85]

134. 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."[86]


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

135. PubMatic also helps advertisers select where to place their ads, to help companies "[s]mash [their] campaign KPIs [key performance indicators]" and "reach [their] target audiences more effectively."[87] 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.[88]

136. In other words, PubMatic utilizes third-party data, as well as data from the publisher 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.

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

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

[86] *Id.*

[87] *Connect With PubMatic's Auction Packages*, PUBMATIC, https://pubmatic.com/auction-packages (last visited Jan. 18, 2024).

[88] *Connect With PubMatic's Auction Packages*, PUBMATIC, https://pubmatic.com/auction-packages-apac (last visited Jan. 18, 2024).

140. By way of example, PubMatic sells a "Ramadan Auction Package" that targets consumers who observe Ramadan.[89] This package helps companies target people who have indicated interest in Ramadan Events through consumer behavior, have internet search history such 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."[90]

141. These partnerships, based on the disclosure of sensitive personal information, are monetized through Defendant's Real-Time Bidding Platform and Private Marketplace Program.

1. Real Time Bidding Program

142. PubMatic's RTB Program is its "real-time bidding auction for advertising impressions." RTB allows advertisers to "bid on Publisher Inventory," including "Publisher Inventory accessed by end users on desktop, mobile devices, smart phones, tablets, connected televisions and other devices. Each impression served on the Publisher Inventory through RTB will be subject to an auction where the 'bids' are derived from Demand Partners."[91] This means that PubMatic hosts, organizes or manages a real-time bidding process in which advertisers try to outbid each other to "win" the right to place ads on users' devices.

143. To further entice its customers to utilize PubMatic's RTB process and to make sure the advertising space that PubMatic customers buy results in quantifiable sales of products/services, PubMatic collects detailed information about users who will be served ads through its RTB process. PubMatic admits that users who "visit or use a digital property that uses [PubMatic] technology" have their information collected and stored through the "use and deploy[ment]" of cookies. Through these cookies, which help with "recognizing and tracking browsing behavior," PubMatic helps participants in the RTB process serve targeted ads to users.[92]

[89] *Connect With PubMatic's Auction Packages: Ramadan*, PUBMATIC, https://pubmatic.com/auction-packages-apac (last visited Jan. 18, 2024).

[90] *Id.*

[91] PubMatic Product Descriptions, https://pubmatic.com/legal/program-descriptions/

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

144. This means that PubMatic deploys cookies and other tracking technologies, including its PubMatic Tracker, on third parties' (and its own customers') websites to better understand and profile users. Once this user data is collected, PubMatic encourages the purchase of ad space through its RTB process by promising advertisers that the ads they place on users' devices will be specifically targeted to users' interests. This targeted advertising will in turn lead to increased sales of the advertisers' products and services.

2. Private Marketplace Program

145. Another product that PubMatic offers is its Private Marketplace Program (PMP).

146. PubMatic's PMP is a "proprietary private marketplace utilizing RTB technology which provides for inventory ordering, impression fulfillment and deal management."[93] Through its PMP, PubMatic conducts invite-only auctions between publishers and buyers, who execute a "negotiated deal on specific inventory."[94]

147. Like PubMatic's open RTB process, the selling point of PubMatic's PMP comes from the accuracy and specificity of PubMatic's user data, which allows advertisers to better target their ads.

148. In fact, PubMatic specifically advertises how the PMP allows advertisers the "ability to target specific audiences in real-time."[95]

149. In PubMatic's own depiction of the PMP process, a hypothetical advertiser participating in the PMP claims they are "interested in targeting 20-30 year old males" for their ads.[96] This depiction shows how the PMP process relies on and benefits from PubMatic's collected user data to facilitate targeted advertising.

[93] PubMatic Product Descriptions, https://pubmatic.com/legal/program-descriptions/

[94] *Private Marketplace (PMP) Deals Explained (Infographic)*, PubMatic (Aug. 5, 2015), https://pubmatic.com/blog/private-marketplace-pmp-deals-explained-infographic/

[95] *Id.*

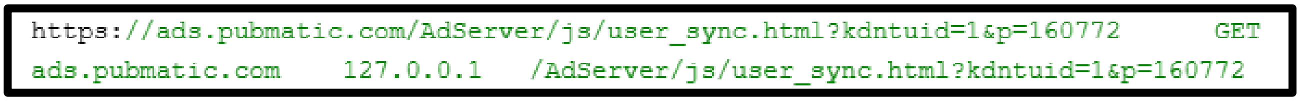
[96] *Id.*

III. DEFENDANT'S COOKIES AND/OR TRACKERS ARE PRESENT ON EACH OF THE SUBJECT WEBSITES

A. Zillow

150. Zillow's website, zillow.com, is an online resource for real estate renters and buyers nationwide. Website visitors can view listings for specific properties, search for properties in specific geographic areas, and apply to rent or buy specific properties.

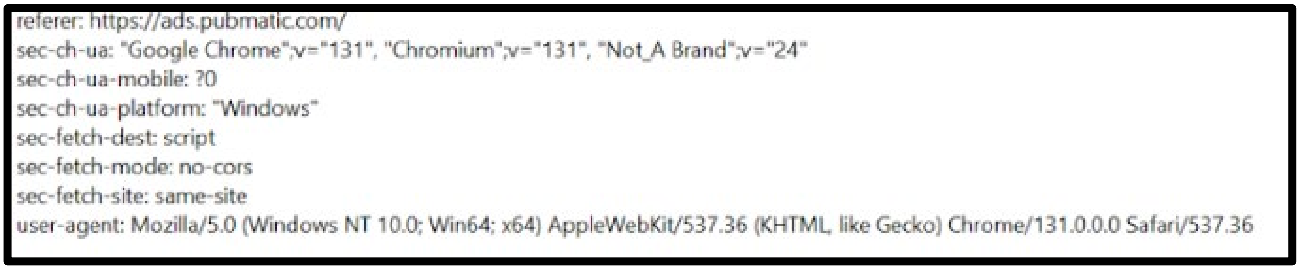
151. Unbeknownst to Zillow Website visitors, the PubMatic Tracker is loaded onto each page the Zillow website.



```
https://ads.pubmatic.com/AdServer/js/user_sync.html?kdntuid=1&p=160772      GET
ads.pubmatic.com    127.0.0.1    /AdServer/js/user_sync.html?kdntuid=1&p=160772
```

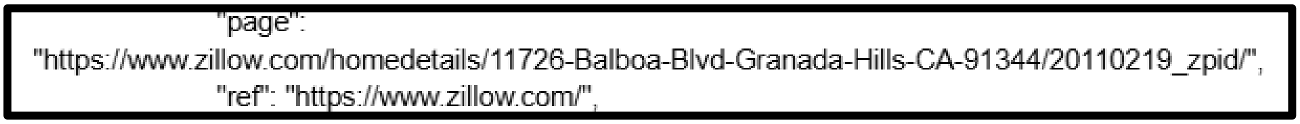
152. As soon as the individual reached the Zillow website, the PubMatic Tracker installs tracking cookies on the individual's browser as described herein.

153. The PubMatic Tracker also collects the individual's browser and device information as described above.



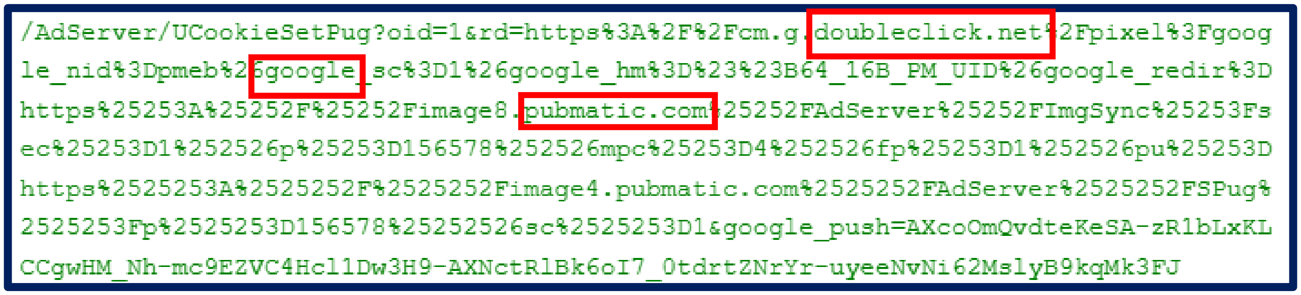
```
referer: https://ads.pubmatic.com/
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-dest: script
sec-fetch-mode: no-cors
sec-fetch-site: same-site
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
```

154. The PubMatic Tracker also gathers the detailed, full-string URL from each page of the Zillow website a user visits, thereby intercepting the user's communications with the website regarding which properties in which geographic areas they want to view.



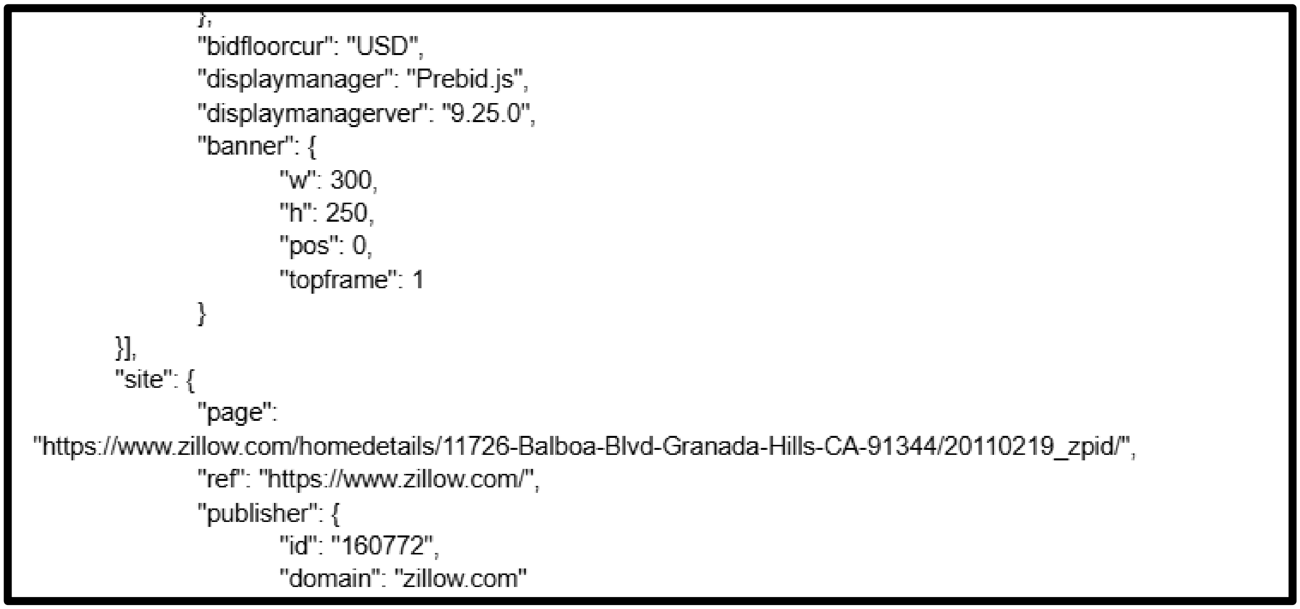
```
                "page":
"https://www.zillow.com/homedetails/11726-Balboa-Blvd-Granada-Hills-CA-91344/20110219_zpid/",
                "ref": "https://www.zillow.com/",
```

155. The Pubmatic Tracker is cookie syncing, providing and receiving identity resolution, and ID matching with numerous Partner Pixels on the Zillow website. The image below shows a sync with the DoubleClick Pixel, owned by Google.



```
/AdServer/UCookieSetPug?oid=1&rd=https%3A%2F%2Fcm.g.doubleclick.net%2Fpixel%3Fgoog
le_nid%3Dpmeb%25google_sc%3D1%26google_hm%3D%23%23B64_16B_PM_UID%26google_redir%3D
https%25253A%25252F%25252Fimage8.pubmatic.com%25252FAdServer%25252FImgSync%25253Fs
ec%25253D1%252526p%25253D156578%252526mpc%25253D4%252526fp%25253D1%252526pu%25253D
https%2525253A%2525252F%2525252Fimage4.pubmatic.com%2525252FAdServer%2525252FSPug%
2525253Fp%2525253D156578%25252526sc%2525253D1&google_push=AXcoOmQvdteKeSA-zR1bLxKL
CCgwHM_Nh-mc9EZVC4Hcl1Dw3H9-AXNctRlBk6oI7_0tdrtZNrYr-uyeeNvNi62MslyB9kqMk3FJ
```

156. This large-scale exchange is in preparation for the real-time servicing of ads on the Zillow website. After collecting (and sharing) as much information as possible on the individual user, Defendant bids on advertising space to target the individual. The image below shows Defendant bidding on a banner ad on the Zillow website.



```
                    },
                    "bidfloorcur": "USD",
                    "displaymanager": "Prebid.js",
                    "displaymanagerver": "9.25.0",
                    "banner": {
                              "w": 300,
                              "h": 250,
                              "pos": 0,
                              "topframe": 1
                    }
          }],
          "site": {
                    "page":
"https://www.zillow.com/homedetails/11726-Balboa-Blvd-Granada-Hills-CA-91344/20110219_zpid/",
                    "ref": "https://www.zillow.com/",
                    "publisher": {
                              "id": "160772",
                              "domain": "zillow.com"
```

157. This type of ad facilitation necessarily involves (i) identifying the website visitor (ii) knowing which page the individual is visiting (*i.e.*, intercepting their selection of articles or other content and (iii) sharing previously gathered information about that individual to make the advertisement more attractive to potential bidders.

158. Defendant then adds this information to its profile on the individual. This profile is connected to the ID assigned to the individual and added to Defendant's data products described herein. This data added to an individual's profile increases its value to advertisers—who can serve ads related to real estate and specific to the geolocations searched to the individual—and enriches

Zillow—as its users are more valuable now that their information is being connected to Defendant's vast repository of information and user profiles.

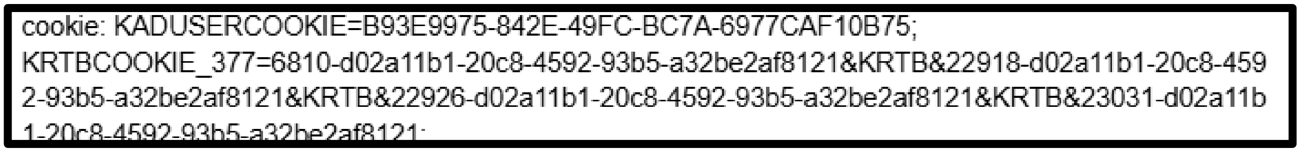
159. Defendant, because of the setting of cookies and collecting of the user's device information and IP address, tracks the future web activity of the individual and adds that information to its consumer profiles and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

B. Peacock

160. Peacock, otherwise known as Peacock TV, is a subscription streaming service featuring films, live sports, and television shows from both NBCUniversal brands and other content providers.

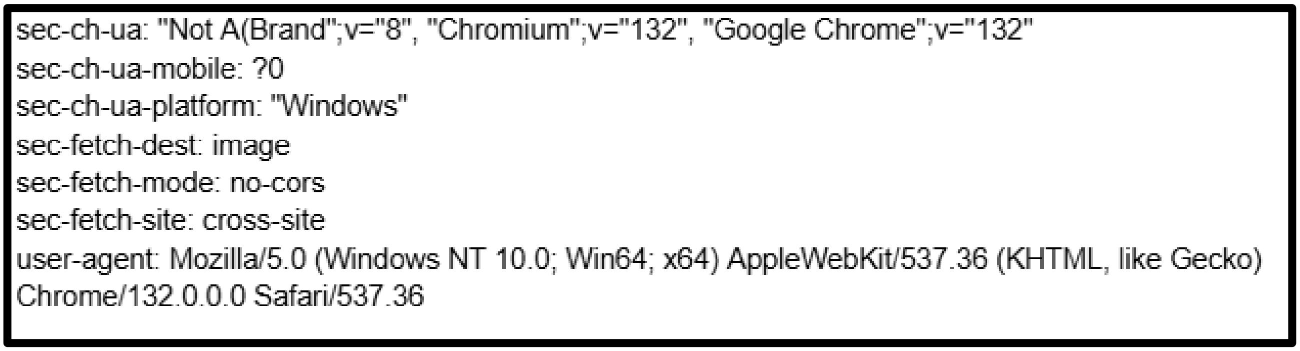
161. Unbeknownst to website visitors, the PubMatic Tracker is loaded onto the Peacock website.

162. As soon as the individual reaches the Peacock website, the PubMatic Tracker installs tracking cookies on the individual's browser in the manner described herein.



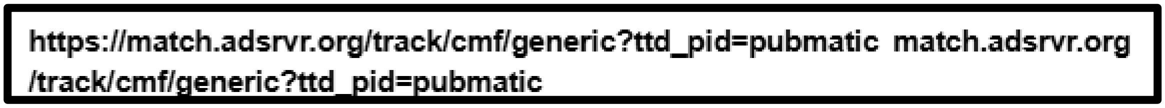
```
cookie: KADUSERCOOKIE=B93E9975-842E-49FC-BC7A-6977CAF10B75;
KRTBCOOKIE_377=6810-d02a11b1-20c8-4592-93b5-a32be2af8121&KRTB&22918-d02a11b1-20c8-459
2-93b5-a32be2af8121&KRTB&22926-d02a11b1-20c8-4592-93b5-a32be2af8121&KRTB&23031-d02a11b
1-20c8-4592-93b5-a32be2af8121;
```

163. The PubMatic tracker also collects device and browser information in the manner described herein.



```
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-dest: image
sec-fetch-mode: no-cors
sec-fetch-site: cross-site
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/132.0.0.0 Safari/537.36
```

164. The PubMatic Tracker is cookie syncing and providing identity resolution to multiple Partner Pixels on the Peacock website.



```
https://match.adsrvr.org/track/cmf/generic?ttd_pid=pubmatic  match.adsrvr.org
/track/cmf/generic?ttd_pid=pubmatic
```

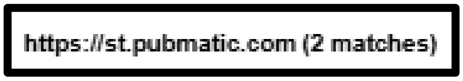
165. Defendant then adds this information to its profile on the individual. This profile is connected to the ID assigned to the individual and added to Defendant's data products described herein. This data added to an individual's profile increases its value to advertisers as its users are more valuable now that their information is being connected to Defendant's vast repository of information and user profiles.

166. Defendant, because of the setting of cookies and collecting of the user's device information and IP address, tracks the future web activity of the individual and adds that information to its consumer profiles and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process

C. Buzzfeed

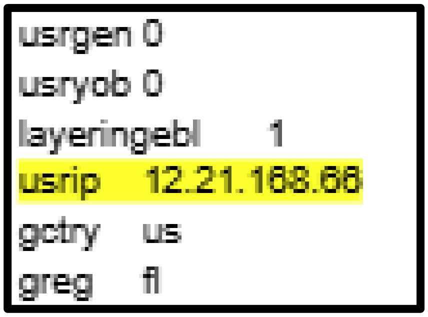
167. Buzzfeed is a popular entertainment and culture website, featuring a variety of articles and quizzes related to popular culture.

168. Unbeknownst to visitors of the Buzzfeed website, the PubMatic Tracker is loaded onto the website.



https://st.pubmatic.com (2 matches)

169. When a user visits the Buzzfeed website, the PubMatic Tracker automatically collects the user's IP address.

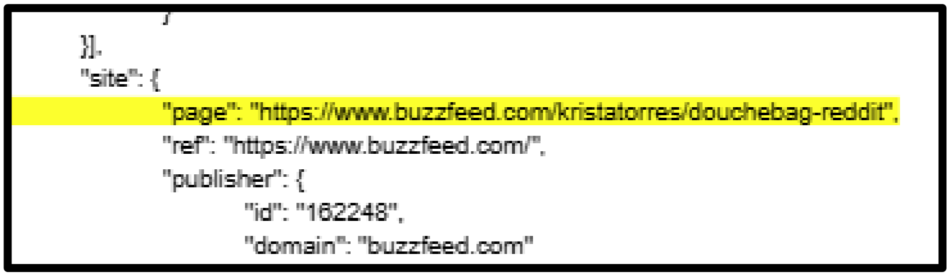


```
usrgen 0
usryob 0
layeringebl     1
usrip    12.21.168.66
gctry    us
greg     fl
```

170. The PubMatic Tracker also immediately loads additional PubMatic cookies onto the individual's browser in the manner described above.

171. Defendant provides identity resolution to dozens Partner Pixels on the Buzzfeed website. The PubMatic Tracker shares both the UID created to track users with the cookies loaded onto their browsers and the user's IP address with each Partner Pixel.

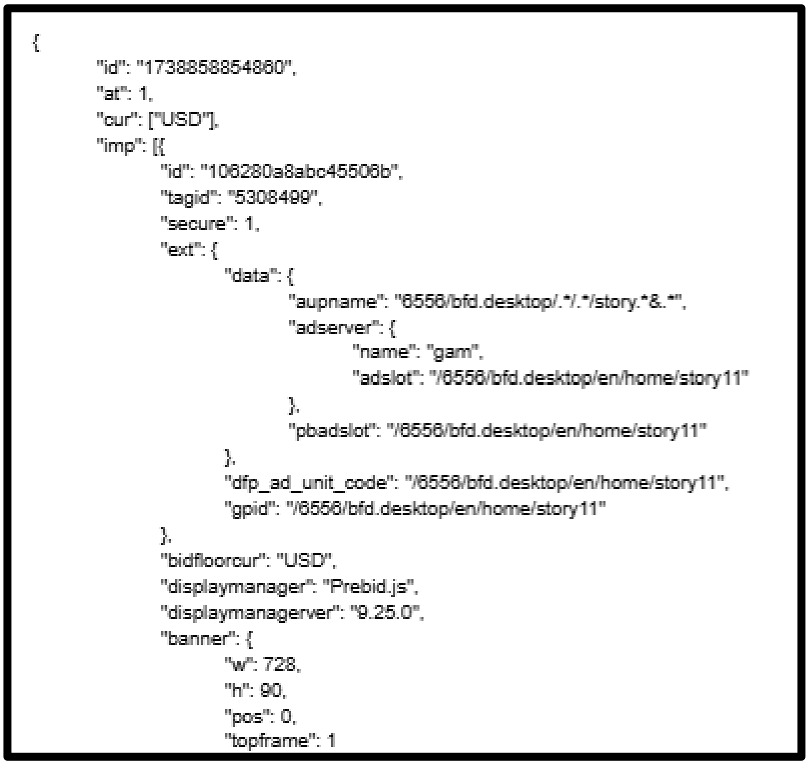
172. Defendant also services real time bidding for advertisements on the Buzzfeed website. To do this, Defendant identifies the user as described above and collects the URL for the page visited by the user as the user clicks on a particular link or article (i.e., in real time).



```
                }
        }],
        "site": {
                "page": "https://www.buzzfeed.com/kristatorres/douchebag-reddit",
                "ref": "https://www.buzzfeed.com/",
                "publisher": {
                        "id": "162248",
                        "domain": "buzzfeed.com"
```

173. Defendant also shares the information it has gathered on a particular user through its PubMatic Tracker to allow bidding partners to know that their advertisements will be targeted to a user's interests.

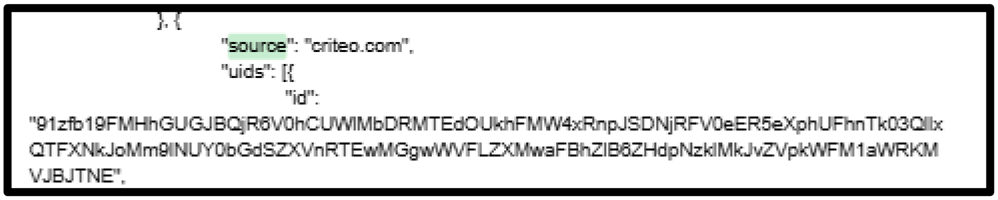
174. Defendant facilitates advertising on specific spaces on the Buzzfeed website. For example, PubMatic operates the advertising space for a banner ad on a particular article published by Buzzfeed.



```
{
        "id": "1738858854860",
        "at": 1,
        "cur": ["USD"],
        "imp": [{
                "id": "106280a8abc45506b",
                "tagid": "5308499",
                "secure": 1,
                "ext": {
                        "data": {
                                "aupname": "6556/bfd.desktop/.*/.*/story.*&.*",
                                "adserver": {
                                        "name": "gam",
                                        "adslot": "/6556/bfd.desktop/en/home/story11"
                                },
                                "pbadslot": "/6556/bfd.desktop/en/home/story11"
                        },
                        "dfp_ad_unit_code": "/6556/bfd.desktop/en/home/story11",
                        "gpid": "/6556/bfd.desktop/en/home/story11"
                },
                "bidfloorcur": "USD",
                "displaymanager": "Prebid.js",
                "displaymanagerver": "9.25.0",
                "banner": {
                        "w": 728,
                        "h": 90,
                        "pos": 0,
                        "topframe": 1
```

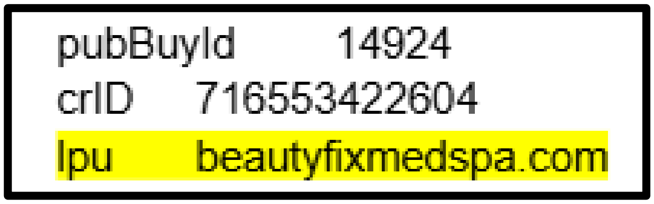
175. Defendant uses the real-time bidding process described above to auction off the ad space to advertisers interested in reaching the particular user, who is identified and profiled by Defendant and the PubMatic Tracker. The image below show that the ad space is available for bidding and the "id" is the unique identifier assigned to a particular user.

176. During the test of the Buzzfeed website, the Partner Pixel Criteo submitted a request to bid on the advertisement, located on the specific Buzzfeed article.



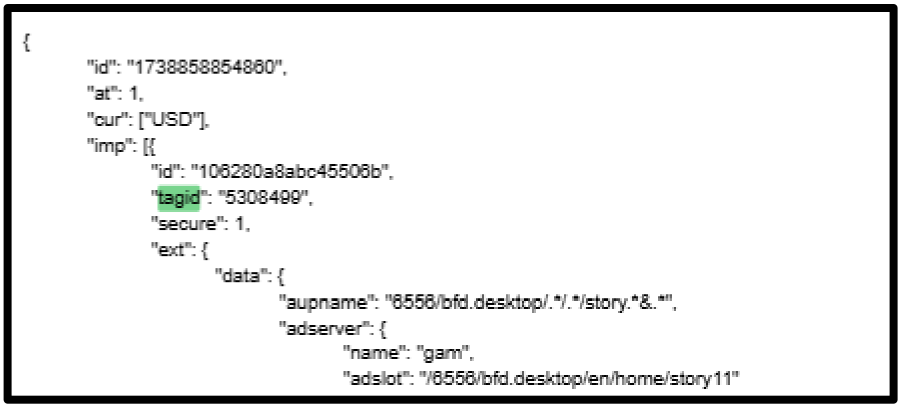
```
                }, {
                        "source": "criteo.com",
                        "uids": [{
                                "id":
"91zfb19FMHhGUGJBQjR6V0hCUWlMbDRMTEdOUkhFMW4xRnpJSDNjRFV0eER5eXphUFhnTk03Qllx
QTFXNkJoMm9lNUY0bGdSZXVnRTEwMGgwWVFLZXMwaFBhZlB6ZHdpNzklMkJvZVpkWFM1aWRKM
VJBJTNE",
```

177. Plaintiffs' testing shows Beauty Fix MedSpa winning the auction to service an advertisement.



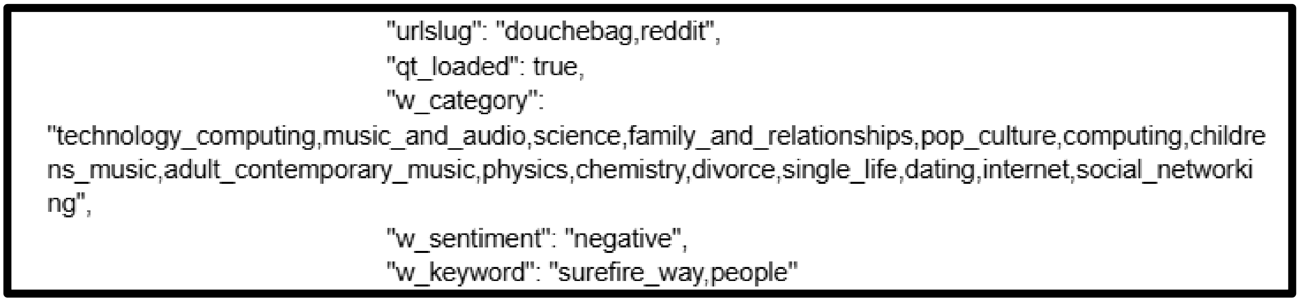
```
pubBuyId     14924
crID    716553422604
lpu     beautyfixmedspa.com
```

178. As with the Zillow and Peacock Websites, the facilitation of advertising space requires the sharing of information about each user with multiple parties who may bid to advertise to that particular user.



```
{
        "id": "1738858854860",
        "at": 1,
        "cur": ["USD"],
        "imp": [{
                "id": "106280a8abc45506b",
                "tagid": "5308499",
                "secure": 1,
                "ext": {
                        "data": {
                                "aupname": "6556/bfd.desktop/.*/.*/story.*&.*",
                                "adserver": {
                                        "name": "gam",
                                        "adslot": "/6556/bfd.desktop/en/home/story11"
```

179. Defendant also collects audience assumptions about the page the user visits, including that the user visited a page with "negative" sentiment and potential topics of interest.



```
                                        "urlslug": "douchebag,reddit",
                                        "qt_loaded": true,
                                        "w_category":
"technology_computing,music_and_audio,science,family_and_relationships,pop_culture,computing,childre
ns_music,adult_contemporary_music,physics,chemistry,divorce,single_life,dating,internet,social_networki
ng",
                                        "w_sentiment": "negative",
                                        "w_keyword": "surefire_way,people"
```

180. Defendant then adds this information to its profile on the individual. This profile is connected to the ID assigned to the individual and added to Defendant's data products described herein. This data added to an individual's profile increases its value to advertisers—who can serve ads related to these keywords, sentiments, and information viewed—and enriches Buzzfeed—as its users are more valuable now that their information is being connected to Defendant's vast repository of information and user profiles.

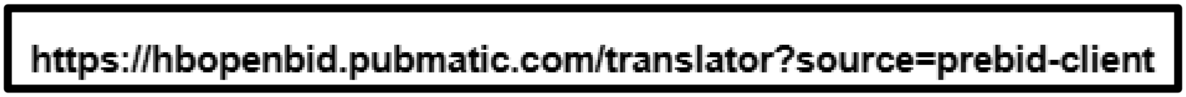
181. Defendant also, because of the setting of cookies and collecting of the user's device information and IP address, tracks the future web activity of the individual and adds that information to its consumer profiles and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

D. Bon Appetit

182. Bon Appetit is a website featuring a wide variety of recipes and related articles about restaurants and food.

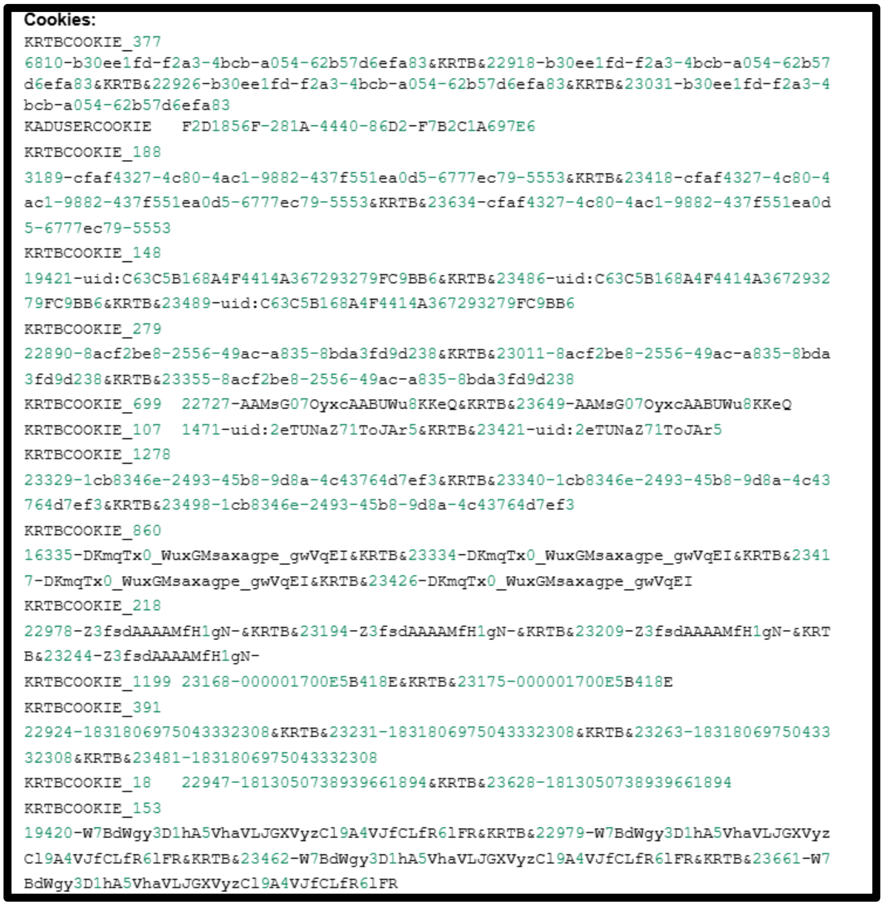
183. The website also contains ad space where companies, like Defendant, facilitate the real-time bidding process to hyper-target advertisements to individual website users based on data collected about their browsing activity and other activity.

184. Unbeknownst to website visitors, the PubMatic tracker is loaded onto each page of the Bon Appetit website.



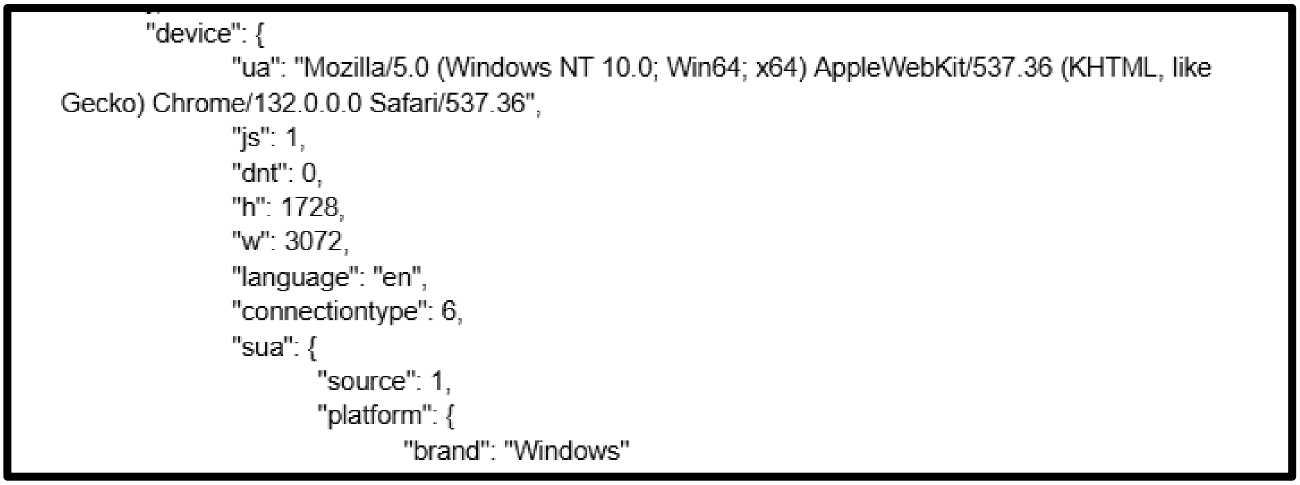
https://hbopenbid.pubmatic.com/translator?source=prebid-client

185. As soon as an individual reaches the Bon Appetit website, the PubMatic Tracker loads tracking cookies on the individual's browser as described herein.



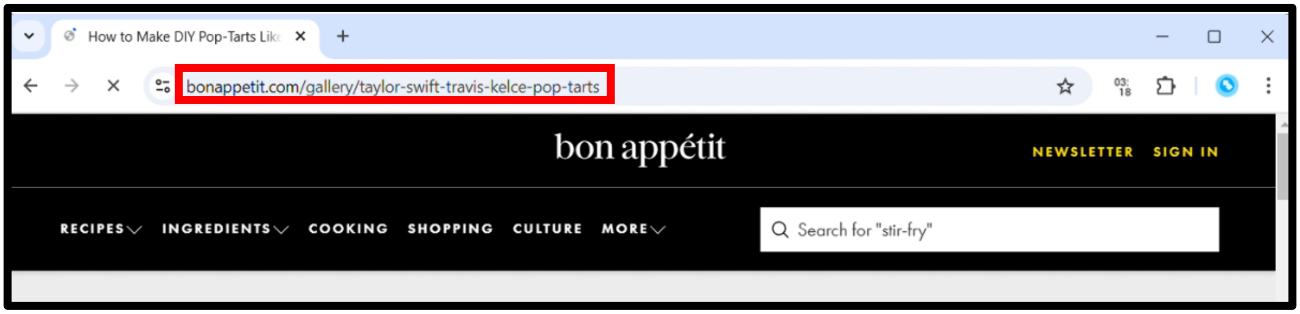
```
Cookies:
KRTBCOOKIE_377
6810-b30ee1fd-f2a3-4bcb-a054-62b57d6efa83&KRTB&22918-b30ee1fd-f2a3-4bcb-a054-62b57
d6efa83&KRTB&22926-b30ee1fd-f2a3-4bcb-a054-62b57d6efa83&KRTB&23031-b30ee1fd-f2a3-4
bcb-a054-62b57d6efa83
KADUSERCOOKIE   F2D1856F-281A-4440-86D2-F7B2C1A697E6
KRTBCOOKIE_188
3189-cfaf4327-4c80-4ac1-9882-437f551ea0d5-6777ec79-5553&KRTB&23418-cfaf4327-4c80-4
ac1-9882-437f551ea0d5-6777ec79-5553&KRTB&23634-cfaf4327-4c80-4ac1-9882-437f551ea0d
5-6777ec79-5553
KRTBCOOKIE_148
19421-uid:C63C5B168A4F4414A367293279FC9BB6&KRTB&23486-uid:C63C5B168A4F4414A3672932
79FC9BB6&KRTB&23489-uid:C63C5B168A4F4414A367293279FC9BB6
KRTBCOOKIE_279
22890-8acf2be8-2556-49ac-a835-8bda3fd9d238&KRTB&23011-8acf2be8-2556-49ac-a835-8bda
3fd9d238&KRTB&23355-8acf2be8-2556-49ac-a835-8bda3fd9d238
KRTBCOOKIE_699  22727-AAMsG07OyxcAABUWu8KKeQ&KRTB&23649-AAMsG07OyxcAABUWu8KKeQ
KRTBCOOKIE_107  1471-uid:2eTUNaZ71ToJAr5&KRTB&23421-uid:2eTUNaZ71ToJAr5
KRTBCOOKIE_1278
23329-1cb8346e-2493-45b8-9d8a-4c43764d7ef3&KRTB&23340-1cb8346e-2493-45b8-9d8a-4c43
764d7ef3&KRTB&23498-1cb8346e-2493-45b8-9d8a-4c43764d7ef3
KRTBCOOKIE_860
16335-DKmqTx0_WuxGMsaxagpe_gwVqEI&KRTB&23334-DKmqTx0_WuxGMsaxagpe_gwVqEI&KRTB&2341
7-DKmqTx0_WuxGMsaxagpe_gwVqEI&KRTB&23426-DKmqTx0_WuxGMsaxagpe_gwVqEI
KRTBCOOKIE_218
22978-Z3fsdAAAAMfH1gN-&KRTB&23194-Z3fsdAAAAMfH1gN-&KRTB&23209-Z3fsdAAAAMfH1gN-&KRT
B&23244-Z3fsdAAAAMfH1gN-
KRTBCOOKIE_1199 23168-000001700E5B418E&KRTB&23175-000001700E5B418E
KRTBCOOKIE_391
22924-1831806975043332308&KRTB&23231-1831806975043332308&KRTB&23263-18318069750433
32308&KRTB&23481-1831806975043332308
KRTBCOOKIE_18   22947-1813050738939661894&KRTB&23628-1813050738939661894
KRTBCOOKIE_153
19420-W7BdWgy3D1hA5VhaVLJGXVyzCl9A4VJfCLfR6lFR&KRTB&22979-W7BdWgy3D1hA5VhaVLJGXVyz
Cl9A4VJfCLfR6lFR&KRTB&23462-W7BdWgy3D1hA5VhaVLJGXVyzCl9A4VJfCLfR6lFR&KRTB&23661-W7
BdWgy3D1hA5VhaVLJGXVyzCl9A4VJfCLfR6lFR
```

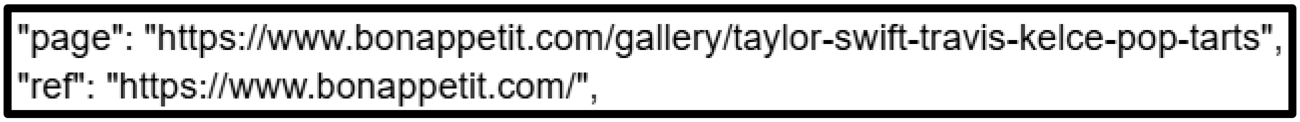
186. The PubMatic tracker also collects the individual's browser and device information as described herein.



```
        "device": {
                "ua": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/132.0.0.0 Safari/537.36",
                "js": 1,
                "dnt": 0,
                "h": 1728,
                "w": 3072,
                "language": "en",
                "connectiontype": 6,
                "sua": {
                        "source": 1,
                        "platform": {
                                "brand": "Windows"
```

187. The PubMatic Tracker also collects the detailed, full-string URL of each page of the Bon Appetit website as the user visits the page (*i.e.* in real time).



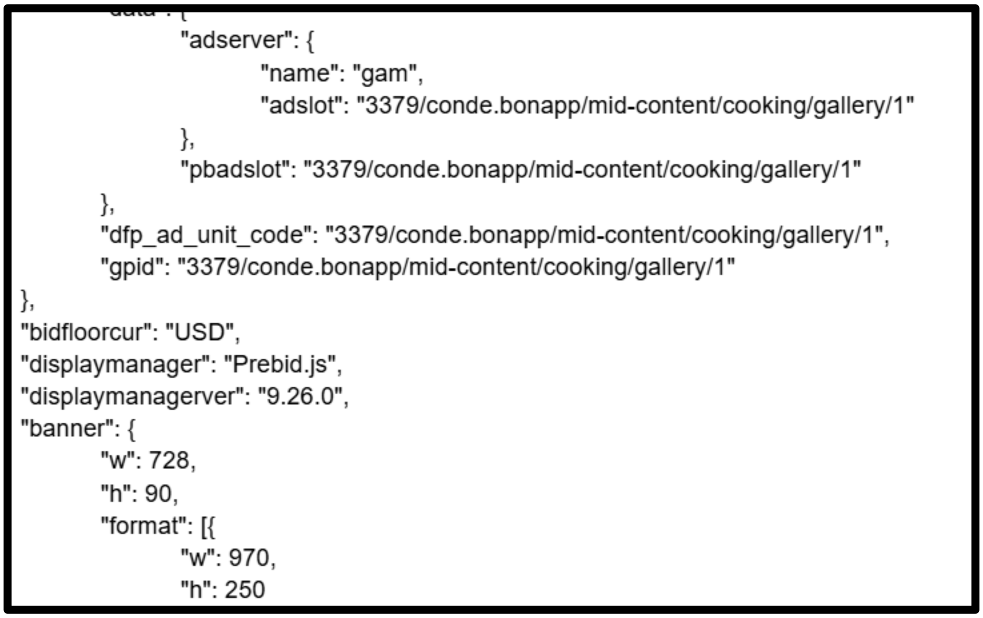


```
"page": "https://www.bonappetit.com/gallery/taylor-swift-travis-kelce-pop-tarts",
"ref": "https://www.bonappetit.com/",
```

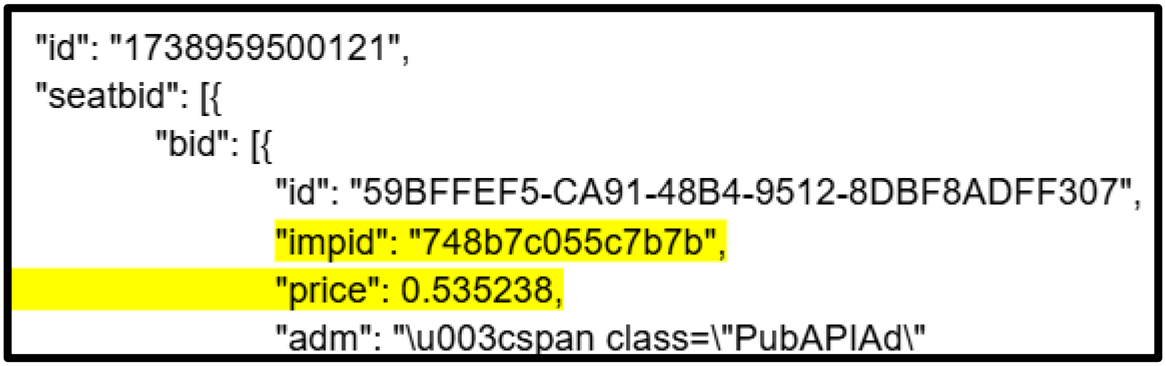
188. The PubMatic Tracker cookie syncs with, provides identity resolution to, and ID syncs with dozens of Partner Pixels on the Bon Appetit website.

189. This massive sharing of data collected on the individual website visitor is done for the purpose of facilitating the real-time bidding auction for targeted advertising on the Bon Appetit website.

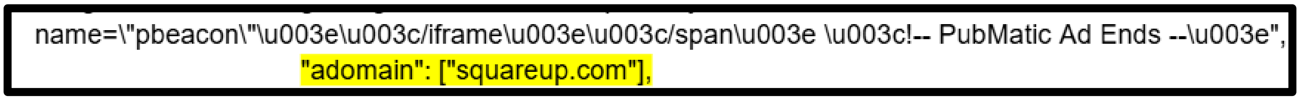
190. Defendant facilitates bidding for a banner ad on the Bon Appetit website. Plaintiffs' testing shows the ad price as $0.53 per thousand impressions and Squareup.com winning the auction for the ad space.



```
                    "data": {
                              "adserver": {
                                        "name": "gam",
                                        "adslot": "3379/conde.bonapp/mid-content/cooking/gallery/1"
                              },
                              "pbadslot": "3379/conde.bonapp/mid-content/cooking/gallery/1"
                    },
                    "dfp_ad_unit_code": "3379/conde.bonapp/mid-content/cooking/gallery/1",
                    "gpid": "3379/conde.bonapp/mid-content/cooking/gallery/1"
          },
          "bidfloorcur": "USD",
          "displaymanager": "Prebid.js",
          "displaymanagerver": "9.26.0",
          "banner": {
                    "w": 728,
                    "h": 90,
                    "format": [{
                              "w": 970,
                              "h": 250
```



```
"id": "1738959500121",
"seatbid": [{
          "bid": [{
                    "id": "59BFFEF5-CA91-48B4-9512-8DBF8ADFF307",
                    "impid": "748b7c055c7b7b",
                    "price": 0.535238,
                    "adm": "\u003cspan class=\"PubAPIAd\"
```



```
name=\"pbeacon\"\u003e\u003c/iframe\u003e\u003c/span\u003e \u003c!-- PubMatic Ad Ends --\u003e",
                    "adomain": ["squareup.com"],
```

191. Defendant then adds this information to its profile on the individual. This profile is connected to the ID assigned to the individual and added to Defendant's data products described herein. This data added to an individual's profile increases its value to advertisers and enriches Bon Appetit—as its users are more valuable now that their information is being connected to Defendant's vast repository of information and user profiles.

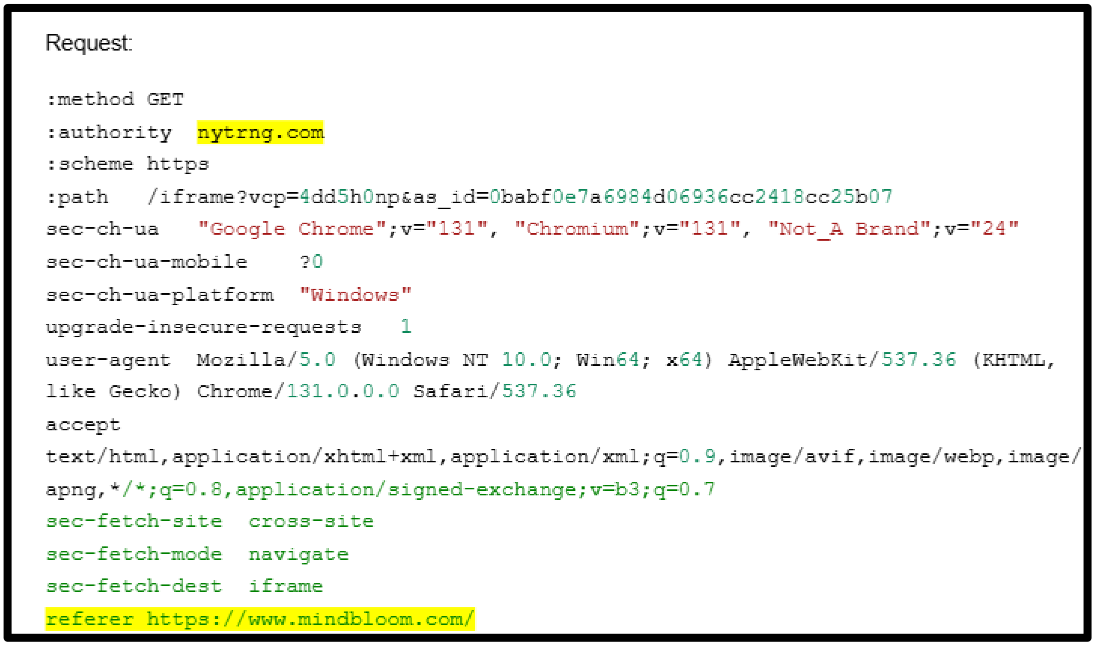
192. Defendant, also, because of the setting of cookies and collecting of the user's device information and IP address, tracks the future web activity of the individual and adds that information to its consumer profiles and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

E. Mindbloom

193. Mindbloom is a medical website offering prescription plans of ketamine therapy for purchase as a treatment for certain mental health conditions, including depression and anxiety.

194. Patients seeking these treatments answer intake questions on the website and can make their purchase if they are approved for a prescription.

195. Unbeknownst to Mindbloom patients, the NYTrng Partner Pixel is loaded onto the Mindbloom website.

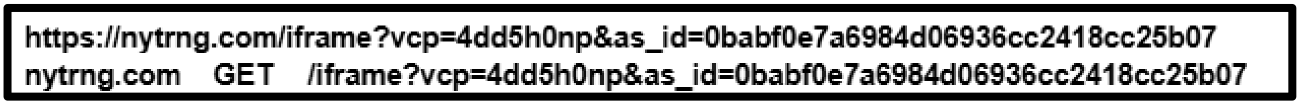


```
Request:

:method GET
:authority  nytrng.com
:scheme https
:path   /iframe?vcp=4dd5h0np&as_id=0babf0e7a6984d06936cc2418cc25b07
sec-ch-ua   "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile    ?0
sec-ch-ua-platform  "Windows"
upgrade-insecure-requests   1
user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/131.0.0.0 Safari/537.36
accept
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
sec-fetch-site  cross-site
sec-fetch-mode  navigate
sec-fetch-dest  iframe
referer https://www.mindbloom.com/
```

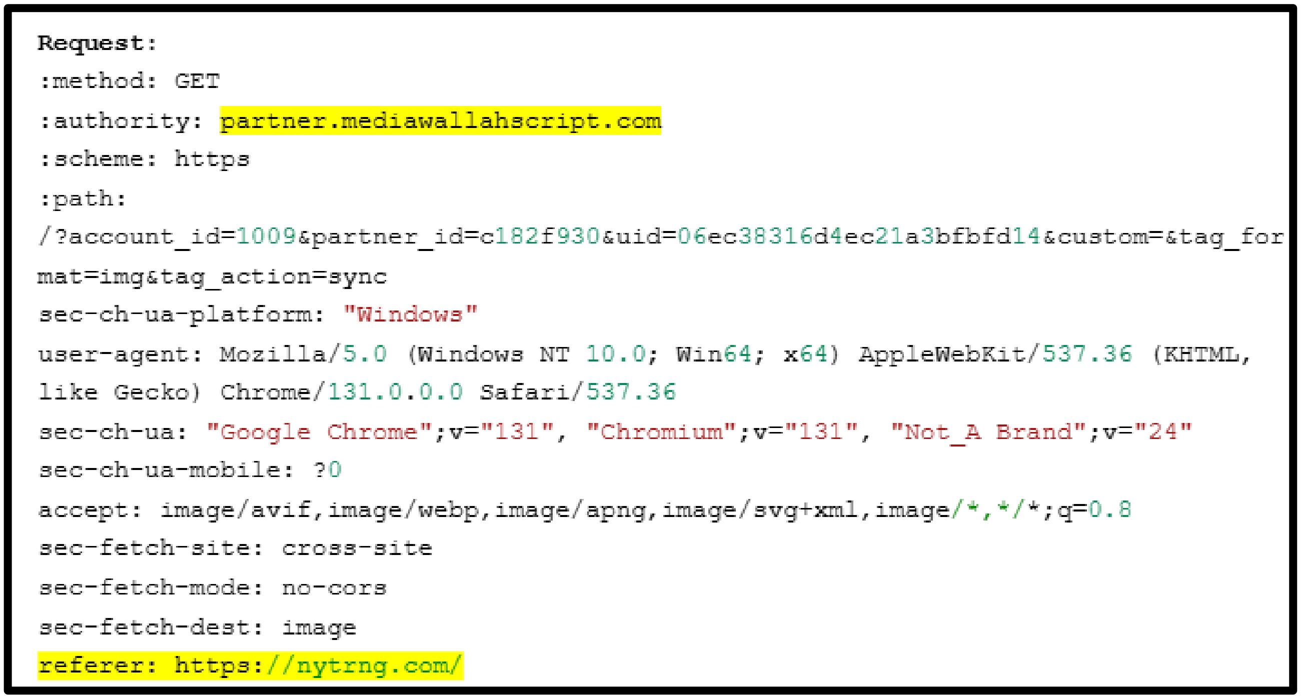
196. As shown in the image above, the NYTrng Pixel collects the URL of the Mindbloom website. This URL is passed to each and every pixel that syncs with either the NYTrng Pixel or any Pixel that has already synced with the NYTrng Pixel. Because Mindbloom only provides ketamine therapy and related services, this information is sufficient to conclude that the individual is seeking ketamine therapy (*i.e.*, information about the individual's confidential medical treatment) and that the individual suffers from a narrow range of mental health conditions for which ketamine therapy is a treatment (confidential information about an individual's medical condition).

197. The NYTrng Pixel initiates a web of cookie syncing and identity resolution by calling over a dozen Partner Pixels onto the Mindbloom website. This is happening through an "iframe." Short for "inline frame," an iframe is an HTML element that allows you to embed another HTML document, webpage, or other content (like videos or maps) within the current page. In plain language, this means the NYTrng Pixel is loading these various pixels into the code of the Mindbloom website.



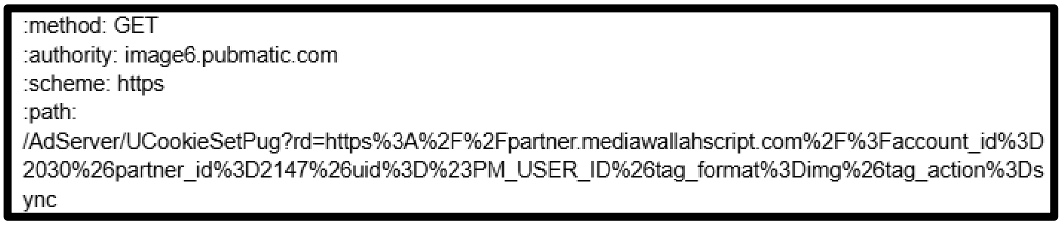
```
https://nytrng.com/iframe?vcp=4dd5h0np&as_id=0babf0e7a6984d06936cc2418cc25b07
nytrng.com   GET   /iframe?vcp=4dd5h0np&as_id=0babf0e7a6984d06936cc2418cc25b07
```

198. One of those Partner Pixels is the Mediawallah Pixel. The NYTrng Pixel and Mediawallah Pixel cookie sync and provide identity resolution regarding the individual website user to each other after the Mediawallah pixel is called onto the Mindbloom website.



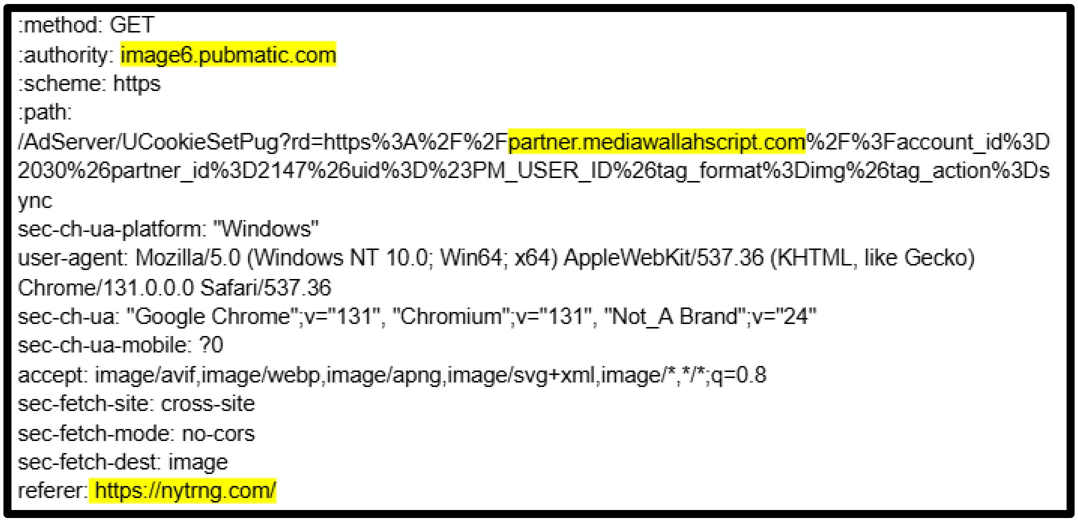
```
Request:
:method: GET
:authority: partner.mediawallahscript.com
:scheme: https
:path:
/?account_id=1009&partner_id=c182f930&uid=06ec38316d4ec21a3bfbfd14&custom=&tag_for
mat=img&tag_action=sync
sec-ch-ua-platform: "Windows"
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/131.0.0.0 Safari/537.36
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
sec-fetch-site: cross-site
sec-fetch-mode: no-cors
sec-fetch-dest: image
referer: https://nytrng.com/
```

199. Milliseconds after receiving the information collected by the NYTrng Pixel, the Mediawallah Pixel cookie syncs and trades identity resolution with Defendant by calling the PubMatic Tracker onto the Mindbloom website.



```
:method: GET
:authority: image6.pubmatic.com
:scheme: https
:path:
/AdServer/UCookieSetPug?rd=https%3A%2F%2Fpartner.mediawallahscript.com%2F%3Faccount_id%3D
2030%26partner_id%3D2147%26uid%3D%23PM_USER_ID%26tag_format%3Dimg%26tag_action%3Ds
ync
```

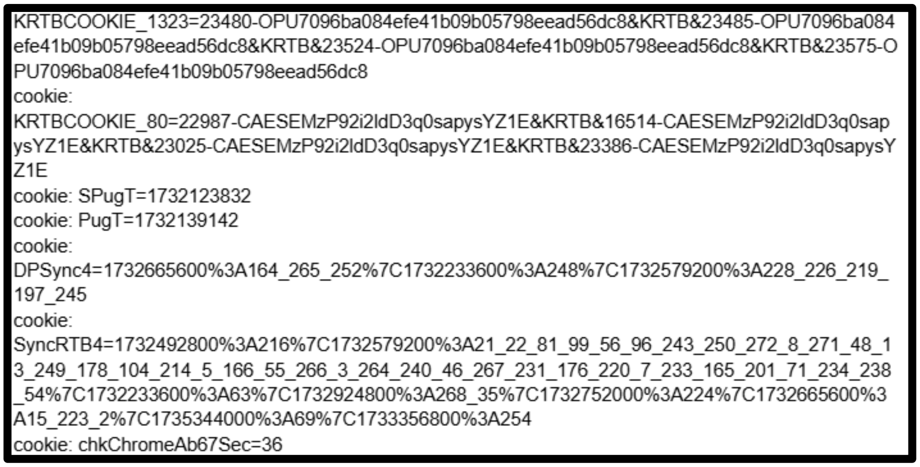
200. Plaintiffs’ testing shows evidence that this is a chain of ID syncing, where each ID sync is shared with the next pixel. For example, the PubMatic Tracker, which only syncs directly with the Mediawallah Pixel, shows the NYTrng Pixel as the referrer for the syncing request.



```
:method: GET
:authority: image6.pubmatic.com
:scheme: https
:path:
/AdServer/UCookieSetPug?rd=https%3A%2F%2Fpartner.mediawallahscript.com%2F%3Faccount_id%3D
2030%26partner_id%3D2147%26uid%3D%23PM_USER_ID%26tag_format%3Dimg%26tag_action%3Ds
ync
sec-ch-ua-platform: "Windows"
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.0.0 Safari/537.36
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
sec-fetch-site: cross-site
sec-fetch-mode: no-cors
sec-fetch-dest: image
referer: https://nytrng.com/
```

201. As shown above, the PubMatic Tracker also collects device and browser fingerprinting information as described herein.

202. As soon as the PubMatic Tracker is called to the Mindbloom website, it loads multiple tracking cookies onto the individual's browser in the manner described above.



```
KRTBCOOKIE_1323=23480-OPU7096ba084efe41b09b05798eead56dc8&KRTB&23485-OPU7096ba084
efe41b09b05798eead56dc8&KRTB&23524-OPU7096ba084efe41b09b05798eead56dc8&KRTB&23575-O
PU7096ba084efe41b09b05798eead56dc8
cookie:
KRTBCOOKIE_80=22987-CAESEMzP92i2IdD3q0sapysYZ1E&KRTB&16514-CAESEMzP92i2IdD3q0sap
ysYZ1E&KRTB&23025-CAESEMzP92i2IdD3q0sapysYZ1E&KRTB&23386-CAESEMzP92i2IdD3q0sapysY
Z1E
cookie: SPugT=1732123832
cookie: PugT=1732139142
cookie:
DPSync4=1732665600%3A164_265_252%7C1732233600%3A248%7C1732579200%3A228_226_219_
197_245
cookie:
SyncRTB4=1732492800%3A216%7C1732579200%3A21_22_81_99_56_96_243_250_272_8_271_48_1
3_249_178_104_214_5_166_55_266_3_264_240_46_267_231_176_220_7_233_165_201_71_234_238
_54%7C1732233600%3A63%7C1732924800%3A268_35%7C1732752000%3A224%7C1732665600%3
A15_223_2%7C1735344000%3A69%7C1733356800%3A254
cookie: chkChromeAb67Sec=36
```

203. Defendant then adds this information to its profile on the individual. This profile is connected to the ID assigned to the individual and added to Defendant's data products described herein. This data added to an individual's profile increases its value to advertisers—who can serve ads related to mental health treatment to the individual—and enriches Mindbloom—as its users are more valuable now that their information is being connected to Defendant's vast repository of information and user profiles.

204. Defendant, because of the setting of cookies and collecting of the user's device information and email address, tracks the future web activity of the individual and adds that information to its consumer profiles and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

IV. DEFENDANT'S SERVICES DEANONYMIZE USERS AND ENRICH DEFENDANT, WEBSITE OPERATORS, AND PARTNER PIXELS ALIKE THROUGH REAL-TIME BIDDING AND PROFILING INDIVIDUALS

A. Defendant Combines The Data From All The Subject Websites With Other Data To Deanonymize Users

205. As a result of PubMatic technology being deployed on thousands or millions of websites, Defendant is collecting various forms of PII and web activity records of numerous Americans and selling that data to target advertising.

206. The information collected, on its own, is enough to identify the individual internet user. But this is only the first step in Defendant's practices of dragnet surveillance.

207. Defendant also combines the data from each and every website a person visits with other data collected by its partner advertisers. Further, through PubMatic's user ID syncing processes, PubMatic has access to not only its own information that it tracks from Internet users, but also the information that its partner advertisers track.[97]

208. For example, PubMatic receives user information such as demographic data, geolocation information, user identifiers, personal information and ID syncing data from its partners that is used in connection with PubMatic's ad services.[98]

209. In this way, PubMatic amasses and aggregates Internet users' data and sells it back to its' partner advertisers. According to PubMatic, its clients can seamlessly integrate the data they have collected with PubMatic own's aggregated user data through its product Identity Hub, which "centralize[s]" and "optimize[s] alternative identity approaches for scale and performance."[99]

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

[98] *Id.*

[99] *Identity Management. Delivered.*, PubMatic, https://pubmatic.com/products/identity-hub/.

B. The Partner Pixels Use The Profiles Created By Defendants To Enhance Their Advertising And Analytics Services

210. The data collected by PubMatic is utilized by both Pubmatic and the Partner Pixels to conduct hyper-targeted advertising through the real-time bidding process. *See* Factual Allegations § I.B, *supra*.

211. The PubMatic identity resolution process is a key part of a complex ecosystem of pixels, cookies or trackers that deliver detailed user information to advertisers to increase the efficiency of those advertisements.

212. Further, the delivery of advertisements facilitated by PubMatic, involves the sharing of vast amounts of consumer information with Partner Pixels.

213. When PubMatic shares website visitor information with a Pixel Partner, that partner (i) uses the information provided by PubMatic to add information to its own data and advertising datasets and (ii) shares the identity information with other advertisers during the real-time bidding delivery of advertisements.

214. For ads to be delivered as soon as a website user visits a site, multiple technology companies need access to detailed information about the identity and interests of the individual website visitor.

215. This information is provided by the Partner Pixels, who use Defendant's identity resolution services or advertising services (which they pay for) to create and expand their own datasets, which they in turn disclose to other players in the real-time bidding ecosystem as advertisements are delivered on websites.

216. Each time a user is selected by this network of advertisers to receive an ad, the advertisers "bid" on the user—meaning Defendant or the Partner Pixels are paid for the information they have stored about that user. Millions of these bids are made per day across the Internet, demonstrating the immense value of the data Defendant improperly collects on Plaintiffs and Class Members.

217. As such, the improper collection of vast amounts of data on Plaintiffs and Class Members is done both for Defendant's profit and for the profit of the Partner Pixels.

V. PLAINTIFFS' EXPERIENCES

A. Plaintiff Kirstie Semien

209. In or about February 2025, Plaintiff Kirstie Semien visited the Buzzfeed website while in California.

210. Unbeknownst to Plaintiff Semien, the PubMatic Tracker was loaded onto each page of the website.

211. When Plaintiff Semien visited the Buzzfeed website, The PubMatic Tracker installed multiple separate cookies onto Plaintiff Semien's browser.

212. The PubMatic Tracker collected information about Plaintiff Semien, including the webpages she visited, her IP address, and fingerprint information about her device and browser, among others.

213. Defendant shared Plaintiff Semien's IP address, unique ID, previously collected information, and information about which pages of the Buzzfeed website she visited with every Partner Pixel to which it provided identity resolution through the PubMatic Tracker.

214. Defendant compiled the information it collected into a profile on Plaintiff Semien and added the bolstered profile to its suite of data products described above.

215. Defendant also, by using the cookies loaded onto Plaintiff Semien's browser, tracked her future web browsing activity across the internet and assisted other Partner Pixels in tracking her and wiretapping her communications with websites.

216. Plaintiff Semien was unaware that Defendant was installing trackers on her browser, wiretapping her communications, aiding in the wiretapping of her communications by Partner Pixels, deanonymizing her personal data, or collecting, selling, and disclosing her personal data to advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor could Plaintiff Semien have discovered these facts.

217. Plaintiff Semien did not provide her prior consent to Defendant to install trackers on her browser, wiretap her communications, aid in the wiretapping of her communications, deanonymize her personal data, or collect, sell, and disclose her personal data to advertising

technology companies, other data brokers, or any person or entity doing business with Defendant. Nor did Defendant obtain a court order to do the same.

218. Plaintiff Semien has, therefore, had her privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendant has been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Semien.

B. Plaintiff Gilbert Gaw

219. In or about January 2024, Plaintiff Gilbert Gaw visited the Peacock website while in California.

220. Unbeknownst to Plaintiff Gaw, the PubMatic Tracker was loaded onto each page of the Peacock website.

221. When Plaintiff Gaw visited the Peacock website, the PubMatic Tracker installed multiple separate cookies onto Plaintiff Gaw's browser.

222. The PubMatic Tracker collected information about Plaintiff Gaw, including the webpages he visited, his IP address, and fingerprint information about his device and browser, among others.

223. Defendant shared Plaintiff Gaw's IP address, unique ID, previously collected information, and information about which pages of the Peacock website he viewed with every Partner Pixel to which it provided identity resolution through the PubMatic Tracker.

224. Defendant compiled the information it collected into a profile on Plaintiff Gaw and added the bolstered profile to its suite of data products described above.

225. Defendant also, by using the cookies loaded onto Plaintiff Gaw's browser, tracked his future web browsing activity across the internet and assisted other Partner Pixels in tracking and wiretapping his communications with websites.

226. Plaintiff Gaw was unaware that Defendant was installing trackers on his browser, collecting his IP address, wiretapping his communications, aiding in the wiretapping of his communications by Partner Pixels, deanonymizing his personal data, or collecting, selling, and disclosing his personal data to advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor could Plaintiff Gaw have discovered these facts.

227. Plaintiff Gaw did not provide his prior consent to Defendant to install trackers on his browser, wiretap his communications, aid in the wiretapping of his communications, deanonymize his personal data, or collect, sell, and disclose his personal data to advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor did Defendant obtain a court order to do the same.

228. Plaintiff Gaw has, therefore, had his privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendant has been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Gaw.

C. Plaintiff Michael Selby

229. In or about December 2024, Plaintiff Michael Selby visited the Zillow website while in California and searched for properties.

230. Unbeknownst to Plaintiff Selby, the PubMatic Tracker was each loaded onto each page of the website.

231. The PubMatic Tracker collected information about Plaintiff Selby's device, browser, and tracked him as he navigated through the website.

232. Defendant, by receiving the full-string URL of each page of the website, intercepted Plaintiff Selby's confidential communications with the Zillow website, including his geographic location and the specific properties that Plaintiff Selby clicked on and viewed.

233. These interceptions happened in real time as the information was entered into the Zillow website.

234. Defendant provided each Partner Pixel with identity resolution services so that each Partner Pixel could deanonymize the data it collected on Plaintiff Selby and sell it during the real-time-bidding process.

235. Defendant also sent and received Plaintiff Selby's information for the purpose of servicing an auction for the real-time bidding of advertisements.

236. Defendant compiled the information it collected into a profile on Plaintiff Selby and added the bolstered profile to its suite of data products described above.

237. Defendant also, by using the cookies loaded onto Plaintiff Selby's browser, tracked his future web browsing activity across the internet and assisted other Partner Pixels in tracking him and wiretapping his communications with websites.

238. Plaintiff Selby was unaware that Defendant was installing trackers on his browser, aiding in the wiretapping of his communications, deanonymizing his personal data, or collecting, selling, and disclosing his personal data, including data about his living situation, to advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor could Plaintiff Selby have discovered these facts.

239. Plaintiff Selby did not provide his prior consent to Defendant to install trackers on his browser, aid in the wiretapping of his communications, deanonymize his personal data, or collect, sell, and disclose his personal data, including data about his living situation, to advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor did Defendant obtain a court order to do the same.

240. Plaintiff Selby has, therefore, had his privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendant has been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Selby.

D. Plaintiff Logan Mitchell

241. In or about February 2025, Plaintiff Logan Mitchell visited the Bon Appetit website while in California and selected and read various recipe articles.

242. Unbeknownst to Plaintiff Mitchell, the PubMatic Tracker was loaded onto each page of the website.

243. The PubMatic Tracker collected information about Plaintiff Mitchell's device, browser, and tracked her as she navigated through the website.

244. Defendant, by receiving the full-string URL of each page of the website, intercepted Plaintiff Mitchell's confidential communications with the Bon Appetit website..

245. These interceptions happened in real time as the information was entered into the Bon Appetit website.

246. Defendant provided each and every Partner Pixel with identity resolution services so that those entities could deanonymize the data it collected on Plaintiff Mitchell, bolster its own data profiles and sell his information during the real-time-bidding process.

247. Defendant compiled this information into a profile on Plaintiff Mitchell and added the bolstered profile to PubMatic's suite of data products described above.

248. Defendant also, by using the cookies loaded onto Plaintiff Mitchell's browser, tracked her future web browsing activity across the internet and assisted other Partner Pixels in tracking her and wiretapping her communications with websites.

249. Plaintiff Mitchell was unaware that Defendant was installing trackers in her browser, aiding in the wiretapping of her communications, deanonymizing her personal data, and collecting, selling, and disclosing her personal data, to advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor could Plaintiff Mitchell have discovered these facts.

250. Plaintiff Mitchell did not provide her prior consent to Defendant to install trackers on her browser, aid in the wiretapping of her communications, deanonymize her personal data, or collect, sell, and disclose her personal data, to advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor did Defendant obtain a court order to do the same.

251. Plaintiff Mitchell has, therefore, had her privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendant has been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Mitchell.

E. Plaintiff Jane Doe

252. In or about November 2024, Plaintiff Jane Doe visited the Mindbloom website while in California to find options for ketamine therapy treatment. She had also purchased a ketamine treatment from the Mindbloom website in or about 2021.

253. Unbeknownst to Plaintiff Doe, the NYTrng Pixel was loaded onto each page of the website.

254. When Plaintiff Doe visited the Mindbloom website, the NYTrng Pixel called the Mediawallah Pixel onto the website, which in turn called the Pubmatic Tracker onto the website.

255. Both the Pubmatic Tracker and the Partner Pixels collected information about Plaintiff Doe's device, browser, and tracked her as she navigated through the website.

256. The NYTrng Pixel and, by extension, the PubMatic Tracker, also received the URL of each page of the website Plaintiff Doe visited, allowing all of the parties working with NYTrng to know that Plaintiff Doe sought and purchased prescription ketamine therapy.

257. Defendant provided Mediawallah with identity resolution services so that Mediawallah could deanonymize the data it collected on Plaintiff Doe and sell it during the real-time-bidding process.

258. Defendant also collected information about Plaintiff Doe, including the webpages she visited, her IP address, and fingerprint information about her device and browser, among others.

259. Defendant compiled this information into a profile on Plaintiff Doe and added the bolstered profile to PubMatic's suite of data products described above.

260. Defendant also, by using the cookies loaded onto Plaintiff Doe's browser, tracked her future web browsing activity across the internet and assisted other Partner Pixels in tracking her and wiretapping her communications with websites.

261. Plaintiff Doe was unaware that Defendant was installing trackers on her browser, aiding in the wiretapping of her communications, deanonymizing her personal data, or collecting, selling, and disclosing her personal data, including data about her medication and health status, to advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor could Plaintiff Doe have discovered these facts. Plaintiff Doe did not become aware that she was being tracked on the Mindbloom website and across the internet by Defendant until November 2024.

262. Plaintiff Doe did not provide her prior consent to Defendant to install trackers on her browser, aid in the wiretapping of her communications, deanonymize her personal data, or collect, sell, and disclose her personal data, including data about her medication and health status, to

advertising technology companies, other data brokers, or any person or entity doing business with Defendant. Nor did Defendant obtain a court order to do the same.

263. Plaintiff Doe has, therefore, had her privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendant has been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Doe.

CLASS ALLEGATIONS

264. **Class Definition:** Plaintiffs seek to represent a class of similarly situated individuals defined as follows:

> All persons in the United States whose personal information, communications, or private information, or data derived from their personal information, communications, or private information, was used to create a profile and/or made available for sale or use through Defendant's Real-Time Bidding Program or Private Marketplace Program, or was combined with other identifiers in Defendant's Identity Hub product, and distributed or sold in the process of delivering advertising on websites, mobile applications, or other digital media, or otherwise.

265. **California Subclass**: Plaintiffs also seek to represent a subclass of similarly situated individuals defined as follows:

> All California citizens in the United States whose personal information, communications, or private information, or data derived from their personal information, communications, or private information, was used to create a profile and/or made available for sale or use through Defendant's Real-Time Bidding Program or Private Marketplace Program, or was combined with other identifiers in Defendant's Identity Hub product, and distributed or sold in the process of delivering advertising on websites, mobile applications, or other digital media, or otherwise.

266. The Class and California Subclass shall be collectively referred to as the "Classes," and Members of the Class and Subclass will collectively be referred to as "Class Members," unless it is necessary to differentiate them.

267. Excluded from the Classes are Defendant, any affiliate, parent, or subsidiary of any Defendant; any entity in which any Defendant has a controlling interest; any officer director, or employee of any Defendant; any successor or assign of any Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

268. **Numerosity**. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiffs at this time; however, it is estimated that there are tens or hundreds of millions of individuals in the Classes. The identity of such membership is readily ascertainable from Defendant's records and non-party records, such as those of Defendant's customers and advertising partners.

269. **Typicality**. Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs, like all Class Members, had their information collected and made available for sale by Defendant through the use of comprehensive user profiles compiled about Plaintiffs.

270. **Adequacy**. Plaintiffs are fully prepared to take all necessary steps to represent fairly and adequately the interests of the Classes. Plaintiffs' interests are coincident with, and not antagonistic to, those of the members of the Classes. Plaintiffs are represented by attorneys with experience in the prosecution of class action litigation generally and in the field of digital privacy litigation specifically. Plaintiffs' attorneys are committed to vigorously prosecuting this action on behalf of the members of the Classes.

271. **Commonality/Predominance**. Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

(a) Whether Defendant's acts and practices alleged herein constitute egregious breaches of social norms;

(b) Whether Defendant acted intentionally in violating Plaintiffs' and Class Members' privacy rights under the California Constitution or common law;

(c) Whether Defendant was unjustly enriched as a result of its violations of Plaintiffs' and Class Members' privacy rights; and

(d) Whether Plaintiffs and Class Members are entitled to damages under CIPA or any other relevant statute;

272. **Superiority**: Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiffs know of no special difficulty to that would be encountered by litigating this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

COUNT I
Intrusion Upon Seclusion

273. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

274. Plaintiffs bring this claim individually and on behalf of the Classes against Defendant.

275. Plaintiffs bring this claim pursuant to California law.

276. To state a claim for intrusion upon seclusion "[Plaintiffs] must possess a legally protected privacy interest … [Plaintiffs'] expectations of privacy must be reasonable … [and Plaintiffs] must show that the intrusion is so serious in 'nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms." *Hernandez v. Hillsides, Inc*. 47 Cal. 4th 272, 286-87 (2009).

277. Plaintiffs and Class Members have an interest in: (i) precluding the dissemination and/or misuse of their sensitive, confidential communications and information; and (ii) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to highly intrusive surveillance at every turn.

278. By conducting such widespread surveillance, Defendant intentionally invaded Plaintiffs' and Class Members' privacy rights, as well as intruded upon Plaintiffs' and Class Members' seclusion.

279. Plaintiffs and Class Members had a reasonable expectation that their communications, identities, personal activities, health and other data would remain confidential.

280. Plaintiffs and Class Members did not and could not authorize Defendant to intercept data on every aspect of their lives and activities.

281. The conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

> (a) Defendant engages in widespread data collection and interception of Plaintiffs' and Class Members' internet and app activity, including their communications with websites and apps, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.
>
> (b) Defendant combines the information collected on websites and apps with offline information also gathered on individuals to create the profiles used in the PubMatic products described herein.
>
> (c) Defendant creates comprehensive profiles based on this online and offline data, which violates Plaintiffs' Class Members' common law right to privacy and the control of their personal information.
>
> (d) Defendant sells or discloses these profiles, which contain the data improperly collected about Plaintiffs and Class Members, to an unknown number of advertisers for use in the real-time-bidding process, which likewise violates Plaintiffs' Class Members' common law right to privacy and the control of their personal information.

282. Defendant's amassment of electronic information reflecting all aspects of Plaintiffs' and Class Members' lives into profiles for future or present use is in and of itself a violation of their right to privacy in light of the serious risk these profiles pose to their autonomy.

283. In addition, those profiles are and can be used to further invade Plaintiffs' and Class Members' privacy by, for example, allowing third parties to learn intimate details of their lives and target them for advertising, political, and other purposes, as described herein, thereby harming them by selling this data to advertisers and other data brokers without their consent.

284. Accordingly, Plaintiff and Class and California Subclass Members seek all relief available for invasion of privacy claims under common law.

COUNT II
Violation Of The California Invasion of Privacy Act
Cal. Penal Code § 631(a)

285. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

286. Plaintiffs bring this claim individually and on behalf of the California Subclass against Defendant.

287. The California Legislature enacted the 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.

288. The California Supreme Court has repeatedly stated the "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas*, 38 Cal. 3d at 363 (emphasis added, internal quotations omitted). This restriction is based on the "substantial distinction … 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." *Id.* at 361 (emphasis added). Such "simultaneous dissemination" "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." *Id.*; *see also Reporters Committee for Freedom of Press*, 489 U.S. at 763 ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

289. Further, "[t]hough written in terms of wiretapping, Section 631(a) applies to Internet communications." *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022). Indeed, "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). This accords with the fact that "the California Supreme Court has [] emphasized that all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purposes of CIPA." *Javier*, 2022 WL 1744107, at *2. "Thus, 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).

290. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

291. To avoid liability under CIPA § 631(a), a defendant must show it had the consent of *all* parties to a communication, and that such consent was procured *prior to* the interception occurring. *See Javier*, 2022 WL 1744107, at *2.

292. Defendant's various cookies, trackers and SDKs, including the PubMatic Tracker, are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

293. Defendant is a "separate legal entity that offers [a] 'software-as-a-service' and not merely [] passive device[s]." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, Defendant has the capability to use the wiretapped information for a purpose other than simply recording the communications and providing the communications to website operators. Accordingly, Defendant was a third party to any communication between Plaintiffs and California Subclass Members, on the one hand, and any of the websites at issue, on the other. *Id*. at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

294. At all relevant times, Defendant willfully and without the consent of all parties to the communication, and in an unauthorized manner, read, attempted to read, and learned the contents of the electronic communications of Plaintiffs and California Subclass Members, on the one hand, and the websites at issue, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

295. At all relevant times, Defendant uses those intercepted communications, including but not limited to building comprehensive user profiles that are offered for disclosure or sale in real-time bidding to prospective advertisers.

296. Further, Defendant "[a]ids, agrees with, employs, or conspires with" each Partner Pixel that it provides identity resolution to and who intercepts Plaintiffs' and California subclass Members' confidential communications.

297. Plaintiffs and California Subclass Members did not provide their prior consent to Defendant's intentional interception, reading, learning, recording, collection, and usage of Plaintiffs' and California Subclass Members' electronic communications.

298. The wiretapping of Plaintiffs and California Subclass Members occurred in California, where Plaintiffs and California Subclass Members accessed the websites, where Defendant's cookies or trackers were loaded on Plaintiffs' and California Subclass Members'

browsers, and where Defendant routed Plaintiffs' and California Subclass Members' electronic communications to Defendant's servers.

299. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and California Subclass Members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

<u>COUNT III</u>
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 638.51(a)

300. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

301. Plaintiffs bring this claim individually and on behalf of the proposed California Subclass against Defendant.

302. 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."

303. 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).

304. 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(c).

305. 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.

306. For example, if a user sends an email, a "pen register" might record the email address it was sent from, the email address the email was sent to, and the subject line—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, the email address it was sent to, and the subject line—because this is *incoming* information that is being sent to that same user.

307. 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 has advanced, however, courts have expanded the application of these surveillance devices. This, combined with the California Supreme Court's mandate to read provisions of the CIPA broadly to protect privacy rights, has led courts to apply CIPA § 638.50 to internet tracking technologies similar to Defendant's technologies at issue here. *See*, *e.g.*, *Shah v. Fandom, Inc.*, --- F. Supp. 3d ---, 2024 WL 4539577, at *21 (N.D. Cal. Oct. 21, 2024) (finding trackers 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); *Moody v. C2 Educ. Sys. Inc.*, --- F. Supp. 3d ---, 2024 WL 3561367, at *3 (C.D. Cal. July 25, 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 provided by data broker was a "pen register").

308. The PubMatic Tracker that PubMatic installed on Plaintiffs' and California Subclass Members' browsers, to the extent it does not intercept "contents" of communications as defined in CIPA § 631(a), is a "pen register[]" because it is a "device or process" that "capture[s]" the "routing, addressing, or signaling information"—the IP address, geolocation, device information, and other persistent identifiers—from the electronic communications transmitted by Plaintiffs' and California Subclass Members' computers or smartphones. Cal. Penal Code § 638.50(b); *see also Shah,* 2024 WL 4539577, at *3; *Mirmalek*, 2024 WL 4102709, at *3.

309. At all relevant times, Defendant installed the PubMatic Tracker—which is a pen register—on Plaintiffs' and California Subclass Members' browsers, which enabled Defendant to collect Plaintiffs' and California Subclass Members' IP addresses, geolocation, device information,

and other persistent identifiers from the websites they visited. Defendant then used the cookies or trackers to build comprehensive user profiles, which were used to unjustly enrich Defendant and its clients by linking and enhancing Plaintiffs' and California Subclass Members' data when it is provided to advertisers through the real-time bidding process.

310. Plaintiffs and California Subclass Members did not provide their prior consent to Defendant's installation or use of the cookies or any other tracking technology at issue.

311. Defendant did not obtain a court order to install or use the cookies or other tracking technology at issue.

312. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and California Subclass 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).

COUNT IV
Unjust Enrichment

313. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

314. Plaintiffs bring this claim individually and on behalf of the Class against Defendant and on behalf of the California Subclass against Defendant.

315. In both cases, Plaintiffs bring this claim pursuant to California law.

316. Defendant has wrongfully and unlawfully trafficked in the named Plaintiffs' and Class Members' personal information and other personal data without their consent for substantial profits.

317. Plaintiffs' and Class Members' personal information and data have conferred an economic benefit on Defendant, which was collected and used by Defendant without consent.

318. Defendant has been unjustly enriched at the expense of Plaintiffs and Class Members, and has unjustly retained the benefits of its unlawful and wrongful conduct.

319. It would be inequitable and unjust for Defendant to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

320. Plaintiffs and Class Members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Defendant obtained as a result of its unlawful and wrongful conduct.

321. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant.

322. Defendant has been unjustly enriched by virtue of its violations of Plaintiffs' and California Class members' legally protected rights to privacy as alleged herein, entitling Plaintiffs and California Class members to restitution of Defendant's enrichment. "[T]he consecrated formula 'at the expense of another' can also mean 'in violation of the other's legally protected rights,' without the need to show that the claimant has suffered a loss." RESTATEMENT (THIRD) OF RESTITUTION § 1, cmt. a.

323. Defendant was aware of the benefit conferred by Plaintiffs. Indeed, Defendant's data-brokerage products are premised entirely on the sale of such data to third parties. Defendant therefore acted in conscious disregard of the rights of Plaintiffs and Class and California Subclass Members and should be required to disgorge all profit obtained therefrom to deter Defendant and others from committing the same unlawful actions again.

COUNT V
Violation of the Electronic Communications Privacy Act
18 U.S.C. §§ 2510, *et seq.*

324. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

325. Plaintiffs bring this claim individually and on behalf of the Class against Defendant and on behalf of the California Subclass against Defendant.

326. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

327. The ECPA protects both sending and the receipt of communications.

328. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

329. The transmission of Plaintiffs' website page visits, selections, bookings, appointment information, purchases and persistent identifiers to each website each qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

330. The transmission of this information between Plaintiff and Class members and each website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

331. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

332. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

333. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

334. The following instruments constitute "devices" within the meaning of the ECPA:

(a) The PubMatic Tracker,

(b) And any other tracking code or SDK used by Defendant; and

(c) Each Partner Pixel;

335. Plaintiff and Class Members' interactions with each website are electronic communications under the ECPA.

336. By utilizing the PubMatic Tracker, as described herein, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class members in violation of 18 U.S.C. § 2511(1)(a).

337. Defendant intercepted communications that include, but are not limited to, communications to/from Plaintiff and Class members regarding their health, travel, shopping habits, consumption of media, geolocation, and many more. This confidential information is then added to consumer profiles and monetized for targeted advertising purposes, among other things.

338. By intentionally using, or endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

339. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, intrusion upon seclusion, CIPA, and other state wiretapping and data privacy laws, among others.

340. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, "[t]he association of Plaintiffs' data with preexisting user profiles is a further use of Plaintiffs' data that satisfies [the crime-tort] exception," because it "violate[s] state law, including the [CIPA], intrusion upon seclusion, and invasion of privacy." *Brown v. Google, LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021); *see also Marden v.LMND Medical Group, Inc.*, 2024 WL 4448684, at *2 (N.D. Cal. July 3, 2024); *R.C. v. Walgreen Co.*, 733 F. Supp. 3d 876, 902 (C.D. Cal. 2024).

341. Defendant was not acting under the color of law to intercept Plaintiffs' and Class members' wire or electronic communications.

342. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy. Plaintiff and Class members had a reasonable expectation that Defendant would not intercept their communications and sell their data to dozens of parties without their knowledge or consent.

343. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq*.

344. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiffs seek statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, et seq. under 18 U.S.C. § 2520.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, seek judgment against Defendant, as follows:

(a) For an order certifying the Classes pursuant to Fed. R. Civ. P. 23, naming Plaintiffs as the representatives of the Classes, and naming Plaintiffs' attorneys as Class Counsel to represent the Classes.

(b) For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;

(c) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;

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

(e) For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a trial by jury of all issues so triable.

Dated: April 8, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta (State Bar No. 354768)
Max S. Roberts (*Pro Hac Vice* Forthcoming)
Victoria X. Zhou (*Pro Hac Vice* Forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

mroberts@bursor.com
vzhou@bursor.com

BURSOR & FISHER, P.A.
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: jwilner@bursor.com

Attorneys for Plaintiffs