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
E-mail: 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 Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JORGE HERNANDEZ-MENDOZA, STACY PENNING, LAURA BONETTI, TANISHA DANTIGNAC, JESSICA JU, and ROBERT MASON, individually and on behalf of all others similarly situated,

Plaintiff,

v.

THE TRADE DESK, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

<u>JURY TRIAL DEMANDED</u>

TABLE OF CONTENTS

PAGE

Plaintiffs Jorge Hernandez-Mendoza, Stacy Penning, Laura Bonetti, Tanisha Dantignac, Jessica Ju, and Robert Mason (collectively "Plaintiffs"), bring this action on behalf of themselves and all others similarly situated against Defendant The Trade Desk, Inc. ("Defendant" or "TTD"). Plaintiffs make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to the allegations specifically pertaining to themselves, which are based on personal knowledge.

NATURE OF THE ACTION

1. This class action lawsuit sets forth how the business practices of TTD amounts to a deliberate surveillance of millions of Americans through their activity on the Internet and mobile applications. TTD, through its software products, tracks in real time and records indefinitely the personal information and specific web activity of millions of Americans.

2. This unlawfully collected information is worth billions of dollars to Defendant because it makes up the content of Defendant's Omnichannel Advertising platform, Adsrvr, 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 Jorge Hernandez-Mendoza.*** Plaintiff Jorge Hernandez-Mendoza is a natural person and citizen of California, residing in Hayward, California. Plaintiff Hernandez-Mendoza was in California when he accessed the Grubhub website and had his activity on that website and subsequent activity tracked by Defendant.

5. ***Plaintiff Stacy Penning.*** Plaintiff Stacy Penning is a natural person and citizen of California, residing in El Cerrito, California. Plaintiff Penning 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.

6. ***Plaintiff Laura Bonetti.*** Plaintiff Laura Bonetti is a natural person and citizen of California, residing in Venice, California. Plaintiff Bonetti was in California when she accessed the Bon Appetit website and had her activity on that website and subsequent activity on other websites tracked by Defendant.

7. ***Plaintiff Tanisha Dantignac.*** Plaintiff Tanisha Dantignac is a natural person and citizen of California, residing in Mission Hills, California. Plaintiff Dantignac was in California when she accessed the Expedia website and had her activity on that website and subsequent activity on other websites tracked by Defendant.

8. ***Plaintiff Jessica Ju.*** Plaintiff Jessica Ju is a natural person and citizen of California, residing in Monterey Park, California. Plaintiff Ju was in California when she accessed the Hyatt website and had her activity on that website and subsequent activity on other websites tracked by Defendant.

9. ***Plaintiff Robert Mason.*** Plaintiff Robert Mason is a natural person and citizen of California, residing in San Jacinto, California. Plaintiff Mason was in California when he accessed the Plushcare website and had his activity on that website and subsequent activity on other websites tracked by Defendant.

10. ***Defendant The Trade Desk, Inc.*** is a Nevada corporation with its principal place of business at 42 North Chestnut Street, Ventura, California 93001. Adsrvr is wholly owned by TTD and TTD directs the actions of Adsrvr, uses Adrvr's technology to accomplish the widespread surveillance alleged herein, and has access to all information collected by Adsrvr.

JURISDICTION AND VENUE

11. 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 Defendant.

12. This Court has personal jurisdiction over Defendant because Defendant collected the private information of thousands or millions of people in California, sold that information to advertisers in California—who targeted advertisements to Californians based in part on their location

in California—and profited from the sale of Californians' personal information. Further, Defendant's principal place of business is in California.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to the claim occurred in this District and Plaintiff Penning resides in this District.

FACTUAL ALLEGATIONS

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

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

A. Data Brokers

15. While "[t]here is no single, agreed-upon definition of data brokers in United States law,"[1] 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).

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."[2] 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."[3]

[1] JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS: THREATS TO AMERICAN CIVIL RIGHTS, NATIONAL SECURITY, AND DEMOCRACY 2 (Duke Sanford Cyber Policy Program eds., 2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

[2] *Id.* at 2.

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

17. For instance, as a report by NATO found, data brokers collect two sets of information: "observed and inferred (or modelled)." The former "is data that has been collected and is actual," such as websites visited." Inferred data "is gleaned from observed data by modelling or profiling," meaning what consumers may be *expected* to do. 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."[4]

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."[5] 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."[6]

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."[7]

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.

[4] Henrik Twetman & Gundars Bergmanis-Korats, *Data Brokers and Security*, NORTH ATLANTIC TREATY ORGANIZATION [NATO] STRATEGIC COMMC'NS CTR. OF EXCELLENCE 11 (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[5] SHERMAN, *supra* note 1, at 1.

[6] *Id.*

[7] *Id.* at 9.

> This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements. 59 Many industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services.
>
> …
>
> Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups.[8]

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.[9]

//

//

//

//

//

//

//

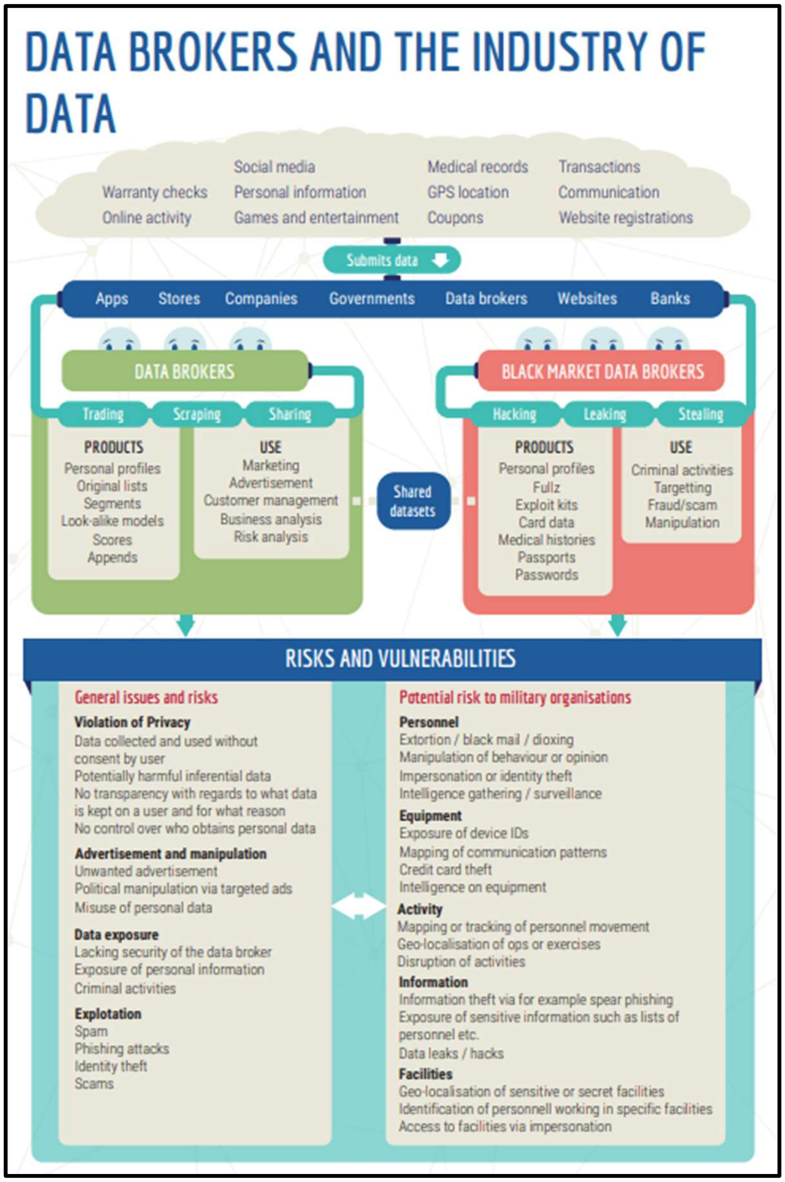
//

//

//

[8] *Id*.

[9] Twetman & Bergmanis-Korats, *supra* note 4, at 8.


DATA BROKERS AND THE INDUSTRY OF DATA
Warranty checks
Online activity
Social media
Personal information
Games and entertainment
Medical records
GPS location
Coupons
Transactions
Communication
Website registrations
Submits data
Apps
Stores
Companies
Governments
Data brokers
Websites
Banks
DATA BROKERS
Trading
Scraping
Sharing
PRODUCTS
Personal profiles
Original lists
Segments
Look-alike models
Scores
Appends
USE
Marketing
Advertisement
Customer management
Business analysis
Risk analysis
Shared datasets
BLACK MARKET DATA BROKERS
Hacking
Leaking
Stealing
PRODUCTS
Personal profiles
Fullz
Exploit kits
Card data
Medical histories
Passports
Passwords
USE
Criminal activities
Targetting
Fraud/scam
Manipulation
RISKS AND VULNERABILITIES
General issues and risks
Violation of Privacy
Data collected and used without consent by user
Potentially harmful inferential data
No transparency with regards to what data is kept on a user and for what reason
No control over who obtains personal data
Advertisement and manipulation
Unwanted advertisement
Political manipulation via targeted ads
Misuse of personal data
Data exposure
Lacking security of the data broker
Exposure of personal information
Criminal activities
Explotation
Spam
Phishing attacks
Identity theft
Scams
Potential risk to military organisations
Personnel
Extortion / black mail / doxing
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

22. Data brokers 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 to track users across the Internet.[10] 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."[11]

[10] *Id.* at 11.

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

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.[12]

24. In short, data brokers 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.

25. Here, TTD's business model functions in the exact same way. As discussed at length below, TTD employs the use of a tracking pixel to track a person's conduct across any device they use that is connected to the internet; meaning their phone, their laptop, and even their smart tv.

26. 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

27. Once data brokers collect information from consumers and create comprehensive user profiles, how do they "sell" or otherwise monetize that information? This is where real-time bidding comes in.

28. "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."[13]

29. "There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs)." An SSP "work[s]

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

[13] Sara Geoghegan, *What is Real Time Bidding?*, ELEC. PRIV. INFO. CTR. (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/.

with website or app publishers to help them participate in the RTB process." "DSPs[,which is what Defendant is,] primarily work with advertisers to help them evaluate the value of user impressions and optimize the bid prices they put forth."[14] 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 ad."[15]

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

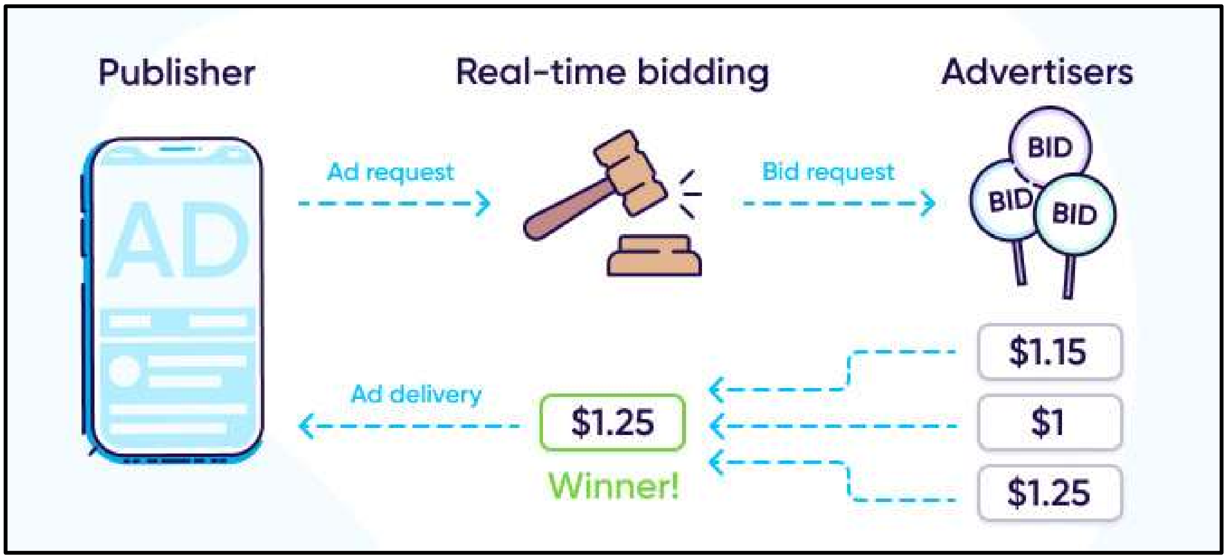
31. The RTB process works as follows:

> 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.[16]

[14] *Id.*

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

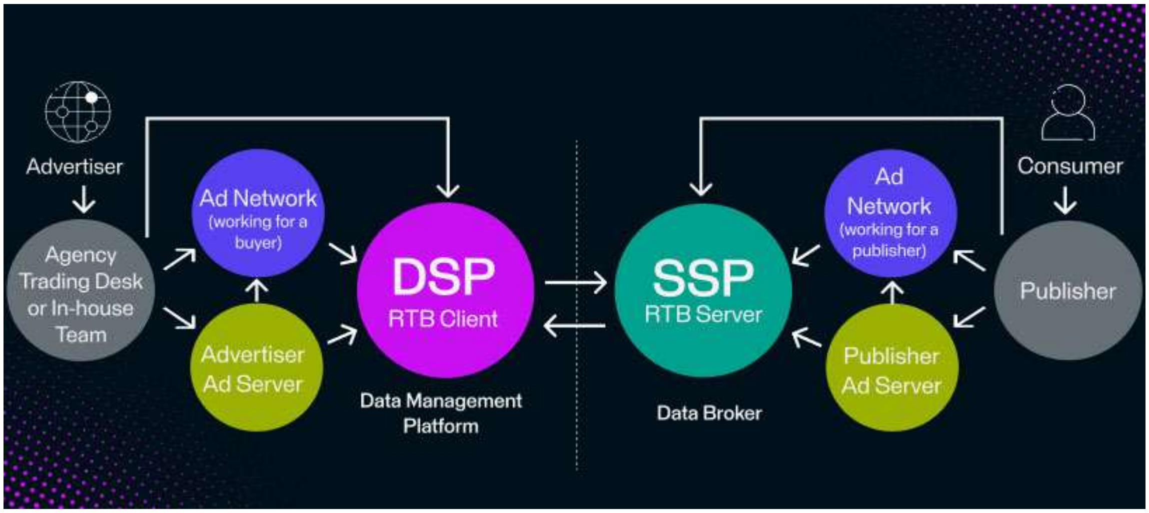
[16] Geoghegan, *supra* note 13; *see also Real-Time Bidding*, APPSFLYER, https://www.appsflyer.com/glossary/real-time-bidding/ (last accessed Feb. 14, 2025).



32. 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:

> 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) [here, Defendants]. 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.[17]

[17] 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/.



33. In other words, before bidding to show a user an advertisement, SSPs and DSPs will attempt to determine what other information about a user may be available. SSPs and DSPs do this by connecting with entities like Defendant, who 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. It also enriches SSPs who can offer users to advertisers for more money based on the greater number of traits available, and DSPs who can receive higher bids for the same users. And SSPs and DSPs can continue linking users on a website or mobile application through the Advertising Exchange, which enhances the SSP's and DSP's ability to better identify users in the future and helps the SSP and DSP profit further as well.

34. Here, Defendant's software functions both as a DSP and a DMP. Meaning that Defendant receives information about what consumer is accessing a website, receives bids from advertisers to put their ads in front of the consumer, and Defendant then enriches the bid by adding TTD's own collection of data on a particular consumer, thereby making the bid worth more because advertisers are more easily able to target a consumer's specific interests. All of this conduct involves significant data sharing with multiple data brokers and online advertisers.

35. 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."[18]

36. The last point bears additional emphasis, as it means the data Defendant uses as a DSP 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.

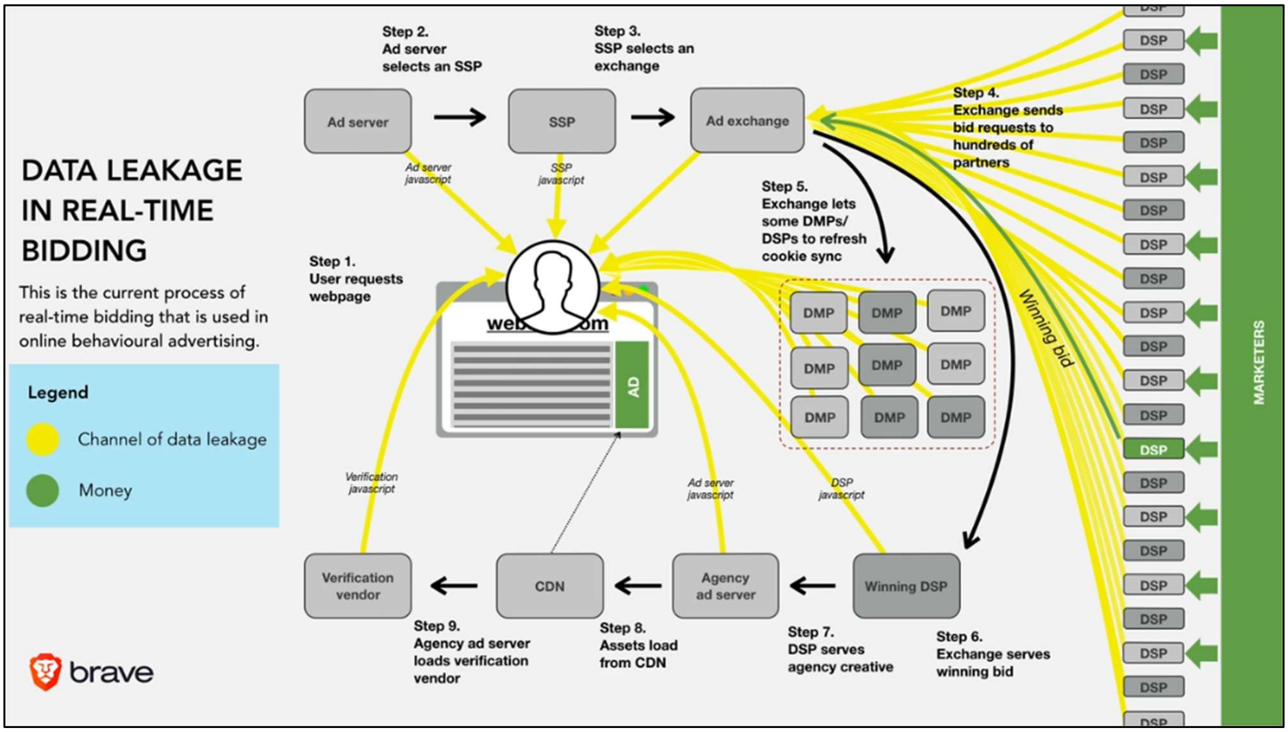
37. Likewise, the Electronic Privacy Information Center ("EPIC") has warned that "[c]onsumers' privacy is violated when entities disclose their information without authorization or in ways that thwart their expectations."[19]

38. For these reasons, some have characterized "real-time bidding" as "[t]he biggest data breach ever recorded" because of the shear number of entities that receive personal information[20]:

[18] F.T.C., UNPACKING REAL TIME BIDDING THROUGH FTC'S CASE ON MOBILEWALLA (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla.

[19] Geoghegan, *supra* note 13.

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



DATA LEAKAGE IN REAL-TIME BIDDING

This is the current process of real-time bidding that is used in online behavioural advertising.

39. 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.").

C. Cookie Syncing

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

41. 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."[21] This allows entities like the Third Parties to circumvent "the restriction that sites can't read each other cookies, in order to better facilitate targeting and real-time bidding."[22]

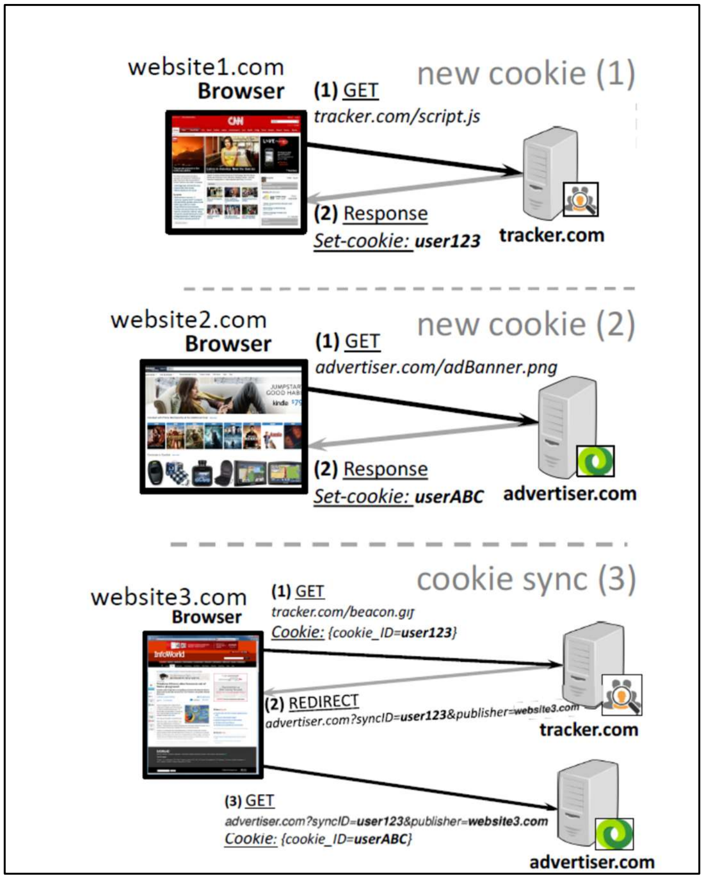
42. Cookie syncing works as follows:

> 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 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.*[23]

[21] 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.

[22] 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)

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



43. 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.[24]

44. On the flip side, "CSync may re-identify web users even after they delete their cookies."[25] "[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."[26] But if a tracker can "respawn" its cookie or like to another persistent identifier (like an IP address), "then through CSync, all of them can link the user's browsing histories from before and after her state erasure. Consequently: (i) users are not able to abolish their assigned userIDs even after carefully erasing their set cookies, and (ii) trackers are enabled to link user's history across state resets."[27]

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

[25] *Id.*

[26] *See id.*

[27] *Id.*

45. Thus, “syncing userIDs of a given user increases the user identifiability while browsing, thus reducing their overall anonymity on the Web.”[28]

46. Cookie syncing is precisely what is happening here. When Defendant’s Pixels are 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.

* * *

47. 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.

48. 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).

49. 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 Defendants 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.

[28] *Id.* at 1441.

50. 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 DEFENDANTS' SERVICES

51. Defendant was founded in 2009 by Jeff Green with the intention of developing technology that would target the same consumer "across ad formats, including display, video, audio, native and social, on a multitude of devices, such as computers, mobile devices, and connected TV."[29]

52. Defendant achieves this through the use of its products: Demand Side Platform, Koa, Data Management Platform, Enterprise APIs,[30] and Galileo.[31]

53. Defendant also increases its capabilities by partnering with over 400 broadcasters, publishers, SSPs, and data collection partners to track and serve advertising to millions of Americans.[32]

A. Defendant's Online Tracking Technology

1. The Adsrvr Pixel

54. Defendant oversees a massive web of online tracking technologies that provide ongoing information to itself and third-party advertisers.

55. The collection of this highly detailed information relies on a "Tracking Tag" "that is placed on a website to track visitor activity on the page...."[33]

[29] *Fact Sheet*, THETRADEDESK, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.thetradedesk.com/assets/general/TTD-Fact-Sheet_121718.pdf (last accessed Feb. 11, 2025).

[30] *Id.*

[31] *Galileo*, THETRADEDESK, https://www.thetradedesk.com/us/our-platform/galileo (last accessed Feb. 14, 2025).

[32] *Our Partners*, THETRADEDESK, https://www.thetradedesk.com/us/our-platform/our-partners (last accessed Feb. 11, 2025).

[33] *Tracking Tags*, THETRADEDESK, https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsOverview (last accessed Feb. 12, 2025).

56. The Tracking Tag that Defendant develops is its ADSRVR pixel that TTD calls a "Universal Pixel."[34]

57. "As its name suggests, the Universal Pixel allows management of multiple processes with just one pixel added to an entire website."[35] "Universal pixels are dynamic and help capture every website visitor no matter what page they're on."[36]

58. As such, Defendant is able to collect information on Internet users' activity on a wide variety of websites through the use of its pixel.

59. The advertisers that Defendant contracts with have their own pixels (the "Partner Pixels"), which are integrated into the design of websites. To facilitate the identity resolution process, described below, these pixels load the ADSRVR pixel owned by TTD onto the website.

60. Plaintiffs' testing has identified dozens of Partner Pixels, but there are likely many more.

61. Specifically, TTD collects information used to identify individuals across the Internet including, but not limited to, cookies, IP addresses, email addresses, HTTP headers that specify information such as type of browser, device and operating system information, location information, and other unique identifiers associated with web addresses.[37] In addition, TTD collects information regarding the users' activity on the websites and communications with the websites in the form of full-string URLs and button click events. Finally, TTD is able to pair this information to any it has otherwise collected about the user and has compiled into a profile of the user that TTD maintains, as alleged below.

[34] *Universal Pixel*, THETRADEDESK, https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsUniversalPixel#universal-pixel-syntax (last accessed Feb. 12, 2025).

[35] *Id.*

[36] *Glossary–Universal Pixel*, THETRADEDESK, https://www.thetradedesk.com/us/glossary#terms-g (last accessed Feb. 14, 2025).

[37] *Id.*

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

2. Interception Of Communications

63. 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.

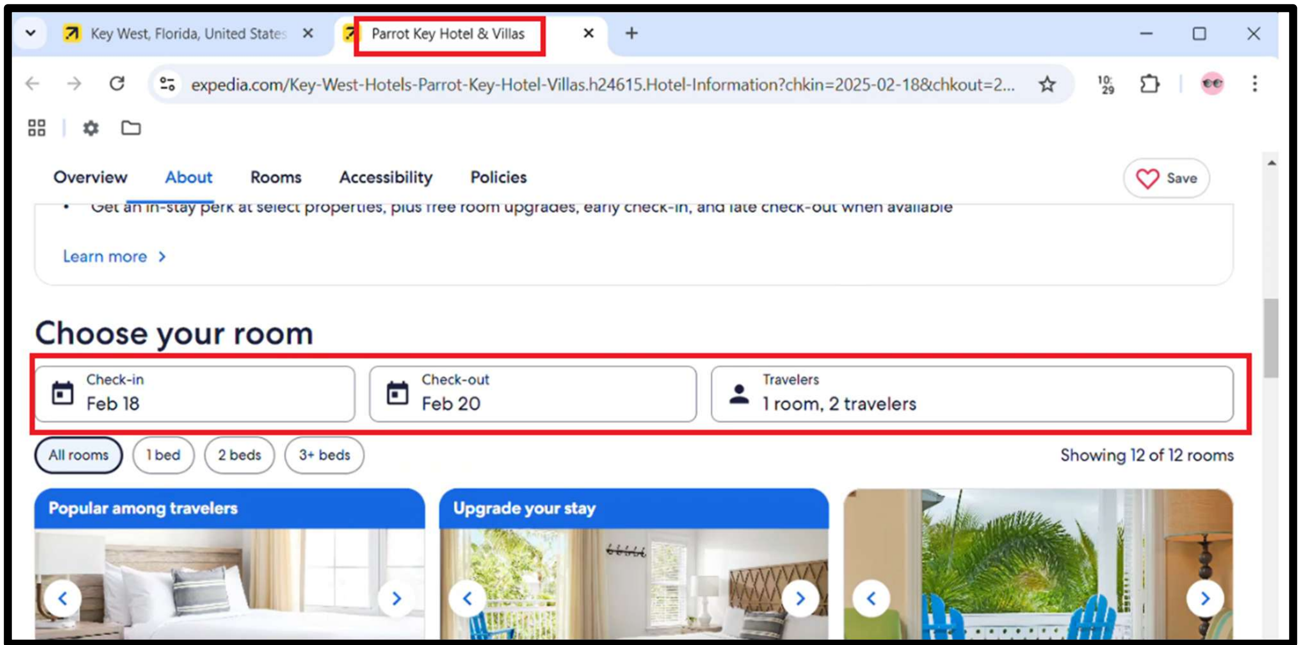
64. When the Adsrvr Pixel is loaded on to a website, Defendant surreptitiously intercepts these communications. The primary way this is accomplished is through the collection of the universal resource locator ("URL") for each page of each website visited by an individual.

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

66. 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.

67. 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.

68. For example, when a user enters information into the Expedia website indicating where they would like to stay and the dates of travel, that information is included in the URL of the webpage with the search results.


Key West, Florida, United States
Parrot Key Hotel & Villas
expedia.com/Key-West-Hotels-Parrot-Key-Hotel-Villas.h24615.Hotel-Information?chkin=2025-02-18&chkout=2...
Overview
About
Rooms
Accessibility
Policies
Save
Learn more
All rooms
1 bed
2 beds
3+ beds
Popular among travelers
Upgrade your stay

• Get an in-stay perk at select properties, plus free room upgrades, early check-in, and late check-out when available

Choose your room

Check-in Feb 18

Check-out Feb 20

Travelers 1 room, 2 travelers

Showing 12 of 12 rooms

https://www.expedia.com/Key-West-Hotels-Parrot-Key-Hotel-Villas.h24615.Hotel-Information?chkin=2025-02-18&chkout=2025-02-20&x_pwa=1&rfrr=HSR&pwa_ts=1738682954508&referrerUrl=aHR0cHM6Ly93d3cuZXhwZWRpYS5jb20vSG90ZWwtU2VhcmNo&useRewards=false&rm1=a2&regionId=1187&destination=Key+West%2C+Florida%2C+United+States+of+America&destType=MARKET&neighborhoodId=864982599800745984&latLong=24.554807%2C-81.802079&sort=RECOMMENDED&top_dp=434&top_cur=USD&userIntent=&selectedRoomType=479195&selectedRatePlan=1856146&searchId=41a0945b-4e2c-4aa1-8923-fa1871205199

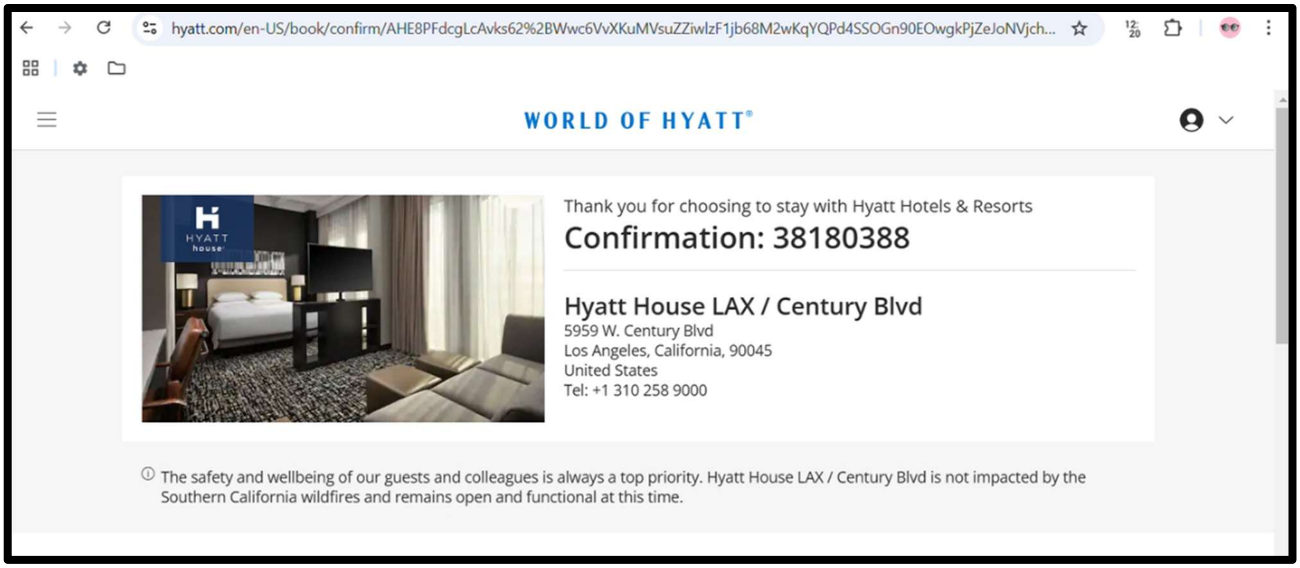
69. The Adsrvr Pixel collects the URL values of the pages visited by millions of internet users and, thus, intercept communications between the individuals and those websites, including sensitive information like travel information and health information.

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

71. The Adsrvr Pixel collects both types of URLs and any information that can be gleaned or inferred from those URLs are added to the profiles that Defendant has for that particular user.

72. The Adsrvr Pixel also intercepts communications between individual internet users and websites that are not contained in the page URL.

73. For example, on the Hyatt website the Adnxs Pixel intercepts booking information from the website itself through a "pageview" event.



hyatt.com/en-US/book/confirm/AHE8PFdcgLcAvks62%2BWwc6VvXKuMVsuZZiwlzF1jb68M2wKqYQPd4SSOGn90EOwgkPjZeJoNVjch...

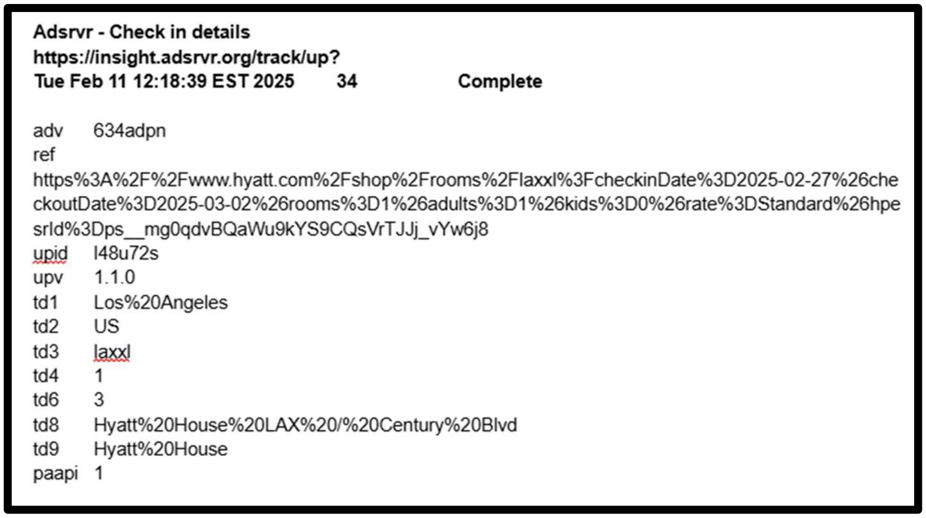
WORLD OF HYATT®

Thank you for choosing to stay with Hyatt Hotels & Resorts

Confirmation: 38180388

Hyatt House LAX / Century Blvd
5959 W. Century Blvd
Los Angeles, California, 90045
United States
Tel: +1 310 258 9000

The safety and wellbeing of our guests and colleagues is always a top priority. Hyatt House LAX / Century Blvd is not impacted by the Southern California wildfires and remains open and functional at this time.



```
Adsrvr - Check in details
https://insight.adsrvr.org/track/up?
Tue Feb 11 12:18:39 EST 2025      34            Complete

adv     634adpn
ref
https%3A%2F%2Fwww.hyatt.com%2Fshop%2Frooms%2Flaxxl%3FcheckinDate%3D2025-02-27%26che
ckoutDate%3D2025-03-02%26rooms%3D1%26adults%3D1%26kids%3D0%26rate%3DStandard%26hpe
srld%3Dps__mg0qdvBQaWu9kYS9CQsVrTJJj_vYw6j8
upid    l48u72s
upv     1.1.0
td1     Los%20Angeles
td2     US
td3     laxxl
td4     1
td6     3
td8     Hyatt%20House%20LAX%20/%20Century%20Blvd
td9     Hyatt%20House
paapi   1
```

74. The Adsrvr Pixel 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.

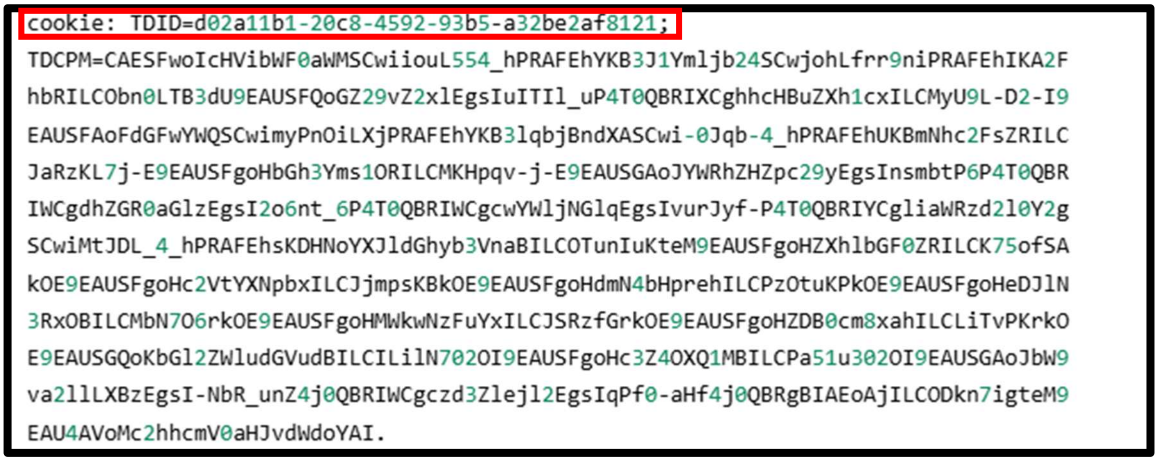
3. *Persistent Identifiers*

75. One way TTD 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. TTD uses these identifiers to confirm that using a particular website is the same person identified by TTD on another website.

76. One form of persistent identifier is a browser "cookie." A cookie is "[a] small file stored by websites on a web user's computer to record data about the user's browsing history."[38]

77. When the Adsrvr Pixel is loaded onto a website, it automatically downloads multiple cookies onto the browser of the person visiting the website. TTD then links a proprietary ID number to the cookie and the individual with the cookie.



```
cookie: TDID=d02a11b1-20c8-4592-93b5-a32be2af8121;
TDCPM=CAESFwoIcHVibWF0aWMSCwiiouL554_hPRAFEhYKB3J1Ymljb24SCwjohLfrr9niPRAFEhIKA2F
hbRILCObn0LTB3dU9EAUSFQoGZ29vZ2xlEgsIuITIl_uP4T0QBRIXCghhcHBuZXh1cxILCMyU9L-D2-I9
EAUSFAoFdGFwYWQSCwimyPnOiLXjPRAFEhYKB3lqbjBndXASCwi-0Jqb-4_hPRAFEhUKBmNhc2FsZRILC
JaRzKL7j-E9EAUSFgoHbGh3Yms1ORILCMKHpqv-j-E9EAUSGAoJYWRhZHZpc29yEgsInsmbtP6P4T0QBR
IWCgdhZGR0aGlzEgsI2o6nt_6P4T0QBRIWCgcwYWljNGlqEgsIvurJyf-P4T0QBRIYCgliaWRzd2l0Y2g
SCwiMtJDL_4_hPRAFEhsKDHNoYXJldGhyb3VnaBILCOTunIuKteM9EAUSFgoHZXhlbGF0ZRILCK75ofSA
kOE9EAUSFgoHc2VtYXNpbxILCJjmpsKBkOE9EAUSFgoHdmN4bHprehILCPzOtuKPkOE9EAUSFgoHeDJlN
3RxOBILCMbN7O6rkOE9EAUSFgoHMWkwNzFuYxILCJSRzfGrkOE9EAUSFgoHZDB0cm8xahILCLiTvPKrkO
E9EAUSGQoKbGl2ZWludGVudBILCILilN702OI9EAUSFgoHc3Z4OXQ1MBILCPa51u302OI9EAUSGAoJbW9
va2llLXBzEgsI-NbR_unZ4j0QBRIWCgczd3Zlejl2EgsIqPf0-aHf4j0QBRgBIAEoAjILCODkn7igteM9
EAU4AVoMc2hhcmV0aHJvdWdoYAI.
```

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

79. After the cookie is loaded onto a person's browser, each time that person visits a website where the Adsrvr Pixel is loaded, TTD uses the cookie to identify the website visitor as the same person who visited previous websites with the same cookie installed on their browser. As such, TTD is able to track each individual internet user across multiple sites to create a more detailed profile on that person's beliefs, interests, and habits.

80. This information is cross-referenced with other information collected by TTD 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.

i. <u>IP Addresses</u>

81. IP addresses are another common persistent identifier.

[38] *Glossary–Cookie*, *supra* note 36.

82. 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.[39]

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

84. 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.

85. 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.[40] Thus, "IP targeting provides a level of specificity and personalization that was never feasible through traditional media or past iterations of digital targeting."[41]

86. An IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[42] and (ii) "to target specific households, businesses[,] and even

[39] *See*, *e.g.*, *What is the Internet Protocol?*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/internet-protocol/ (last accessed Feb. 14, 2025); *What is an RFC1918 Address?*, NETBEEZ, https://netbeez.net/blog/rfc1918/ (last accessed Feb. 14, 2025).

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

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

[42] *Location-Based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/ (last accessed Feb. 14, 2025).

individuals with ads that are relevant to their interests."[43] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[44] because "[c]ompanies can use an IP address … to personally identify individuals."[45]

87. 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 services will appeal to their needs."[46] For example, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.[47]

88. "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."[48]

89. "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."[49]

[43] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert williams-z7bhf.

[44] *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/.

[45] 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/.

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

[47] *See, e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns (last accessed Feb. 14, 2025).

[48] *IP Targeting*, SAVANT DSP, https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB (last accessed Feb. 14, 2025).

[49] *Id.*

90. 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."[50] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[51]

91. In addition, "IP address targeting can help businesses to improve their overall marketing strategy."[52] "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."[53]

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

> [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.[54]

93. 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."[55]

ii. <u>Mobile Advertising Identifiers</u>

94. TTD employs similar methods to track individuals using mobile apps.

[50] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023) https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] Twetman & Bergmanis-Korats, *supra* note 4, at 11.

[55] *Is an IP Address Personal Data?*, CONVESIO, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/ (last accessed Feb. 14, 2025); *see also What Is Personal Data?*, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en (last accessed Feb. 14, 2025).

95. TTD owns and operates multiple "software development kits" (SDKs), pieces of code that work independently or with "application programming interfaces" (APIs) and are loaded into mobile apps and can track users' activity on certain apps.[56]

96. 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."[57]

97. An API "acts 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."[58] An API can "work[] as a standalone solution or included within an SDK … [A]n SDK often contains at least one API."[59] 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."[60]

98. Similar to the Adsrvr Pixel on web browsers, the TTD SDKs are loaded onto apps and track user information when an individual accesses a particular app.

99. The TTD SDKs track the types of user information Defendant obtains through the Adsrvr Pixel including, but not limited to, users': location information, email addresses, device and advertising identifiers, and usage of the particular app being accessed.

100. In addition to its own ID tracking, TTD collects advertising identifiers that are designed to track the app activity of individual users across different apps. Two of the most

[56] *SDK vs. API: What's the Difference*, I.B.M. (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) (last visited Dec. 23, 2024). Plaintiffs will refer to both collectively as the "TTD SDKs" to avoid any confusion.

[57] *API vs. SDK: The Difference Explained (With Examples*), STREAM, https://getstream.io/glossary/api-vs-sdk/ (last accessed Feb. 14, 2025).

[58] *What is an API (Application Programming Interface)?*, I.B.M. (Apr. 09, 2024) https://www.ibm.com/topics/api.

[59] *SDK vs. API: What's the Difference*, *supra* note 56 ("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).

[60] *Application Programming Interface*, SDXCENTRAL, https://www.sdxcentral.com/resources/glossary/application-programmatic-interface-api/ (last accessed Feb. 14, 2025).

prominent are AAIDs (for Android devices) and IDFAs (for iOS devices) (collectively, "Mobile Advertising IDs" or "MAIDs").

101. An AAID is a unique string of numbers which 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 mobile applications.[61] 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.

102. Although technically resettable, an AAID is a persistent identifier because virtually no one knows about AAIDs and, correspondingly, virtually no one resets that identifier. The fact that the use and disclosure of AAIDs is so ubiquitous evinces an understanding on the part of Defendants, Google, and others in the field that they 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 GOVERNMENT 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).

103. Using publicly available resources, an AAID can track a user's movements, habits, and activity on mobile applications.[62] Put together, the AAID serves as "the passport for aggregating all of the data about a user in one place."[63]

104. 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

[61] *Advertising ID*, GOOGLE, https://support.google.com/googleplay/android-developer/answer/6048248 (last accessed Feb. 14, 2025).

[62] 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.

[63] Willie Boag, *Trend Report: Apps Oversharing Your Advertising ID*, INT'L DIGIT. ACCOUNTABILITY COUNCIL. https://digitalwatchdog.org/trend-report-apps-oversharing-your-advertising-id/ (last accessed Feb. 14, 2025).

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.

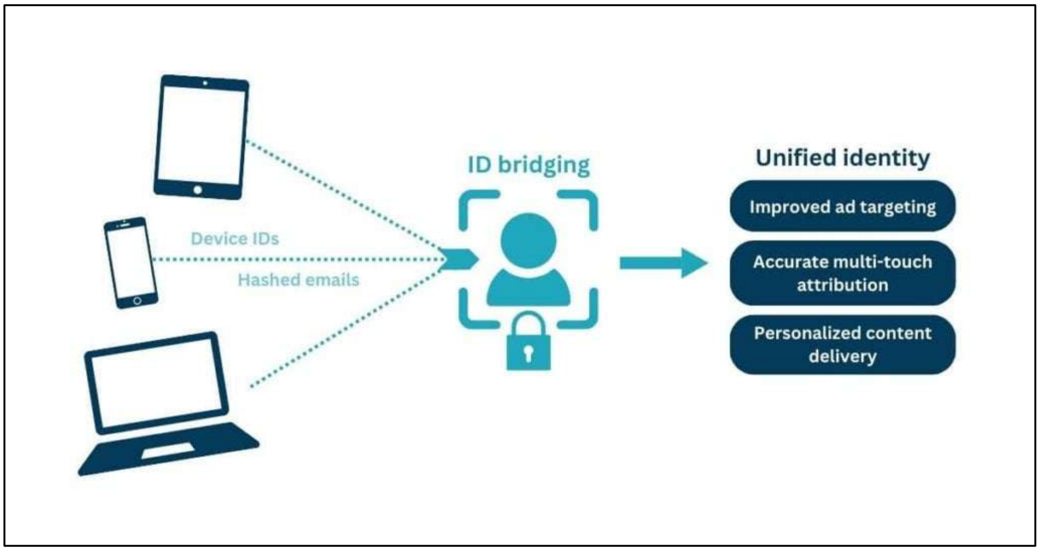
105. Similarly, an "Identifier for Advertisers, or IDFA for short, is a unique, random identifier (device ID) that Apple assigns to every iOS device. An IDFA would be the equivalent of a web cookie, in the sense that it enables advertisers to monitor users' engagement with their ads, and keep track of their post-install activity."[64]

106. As with the ADSRVR pixel and AAID, TTD's collection of IDFAs allows it 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 permits even an ordinary person to identify a specific individual with the IDFA.

107. 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."[65] 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.

[64] *Identifier for Advertisers (IDFA)*, APPSFLYER, https://www.appsflyer.com/glossary/idfa (last accessed Feb. 14, 2025).

[65] Kayleigh Barber, *WTF Is The Difference Between Id Bridging And Id Spoofing?*, DIGIDAY (July 8, 2024), https://digiday.com/media/wtf-is-the-difference-between-id-bridging-and-id-spoofing/.



108. ID Bridging "has long been the foundation of programmatic advertising,"[66] which is the process by which companies "use [] advertising technology to buy and sell digital ads" by "serv[ing] up relevant ad impressions to audiences through automated steps, in less than a second."[67] It entails a "unique identifier[] assigned to individual devices," including "Google's Advertising ID," personal information like geolocation and e-amil address, and "cross-platform linkage."[68]

109. 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."[69]

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

[67] *Programmatic Advertising*, AMAZON ADS, https://advertising.amazon.com/blog/programmatic-advertising# (last accessed Feb. 14, 2025).

[68] Anete Jodzevica, *ID Bridging: The Privacy-First Future of Audience Targeting*, SETUPAD (Nov. 15, 2024), https://setupad.com/blog/id-bridging/. Ironically, the example given in this article is a "hashed e-mail," where the e-mail Defendant collected in this example is not hashed.

[69] 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 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.

111. 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).

112. In February 2019, Oracle published a paper entitled "Google's Shadow Profile: A Dossier of Consumers Online and Real World Life,":

> 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.[70]

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

iii. <u>Other Identifiers</u>

114. In addition to the methods described above, which are explicitly designed to track individuals across different devices and apps, TTD collects other identifying information that allows

[70] ORACLE, GOOGLE'S SHADOW PROFILE: A DOSSIER OF CONSUMERS ONLINE AND REAL WORLD LIFE 1 (2019), https://tinyurl.com/2mtuh7vf.

it to determine whether the same individual is visiting multiple websites or using multiple apps where TTD technology is called to or installed directly.

115. One method is through collecting e-mail addresses. The logic of this is straightforward. If TTD collects the same e-mail address from two different site visits, it can determine with almost total accuracy that the sites are both being visited by the same person. The same is true of devices. If the same e-mail address is captured on two different devices, it is very likely those devices are used by the same individual.

116. Location information functions in a similar manner. If multiple websites or apps are visited from the same location, the pool of potential individuals who are accessing the website or app is narrowed considerably immediately and can be narrowed to a pinpoint over time.

117. HTTP requests, when intercepted by TTD, collect device information that can also identify whether the same user is visiting multiple sites or apps, and can distinguish between the devices being used by a particular person. With every visit, and every subsequent HTTP request, the device information will be identical in each.

4. Identity Resolution

118. In addition to its own tracking of individuals across the internet, TTD sells its tracking services to other advertisers who own and operate pixels through a process known as identity resolution.

119. Identity resolution is the technology marketing term for the process of data tracking described above. As TTD describes it: "identity resolution is the association of pseudonymized digital identifiers at the household and individual level for advertising use cases such as cross-device targeting, post-campaign measurement, and attribution."[71]

120. In plain language, identity resolution is the culmination of TTD'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.

[71] *How Identity Graphs are Built – The Present and the Future*, THETRADEDESK, https://www.thetradedesk.com/us/resource-desk/how-identity-graphs-are-built-the-present-and-the-future (last accessed Feb. 12, 2025).

121. 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.

122. When a Partner Pixel is loaded onto a website, the Adsrvr Pixel (in addition to the independent tracking described above) interacts with the Partner Pixel. Specifically, TTD provides allows those pixels to access the information associated with each individual.

123. With respect to the delivery of targeted advertisements on websites, TTD'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 the Adsrvr Pixel.

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

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

126. 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 TTD. 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*.

127. Specifically, Plaintiffs' counsel found that each website and/or app had Partner Pixels loaded onto it, which in interacted with TTD to better enable their advertising. Partner Pixels would themselves intercept users' communications with the website or app. These Partner Pixels—which contract with Defendant—obtain identity resolution from Defendant to aid or enable this interception. The Adsrvr Pixel would then assign an 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 TTD collected and provided to the Partner Pixels.

5. *The Trade Desk's Data Profile Products*

128. TTD gathers first-party data such as names, physical addresses, email addresses, mobile ad identifiers (MAIDs), IP addresses, and other information to link economic transactions to a specific consumer ID.[72]

129. In addition to collecting and aggregating information on millions of people, TTD tracks many of those same people to sell decision analytic and marketing assistance to businesses, including individual fingerprinting and targeting for advertising.

130. TTD's pool of information is used to make detailed profiles on the web and purchase habits of nearly every American, are constantly updated by the widespread tracking of individuals across the internet.

131. TTD has access to all the data collected by the Adsrvr Pixel and SDKs described above. This, however, is not the totality of TTD's data. TTD also obtains data from other surveillance projects, from third parties it contracts with to receive information, and from publicly available sources.[73]

132. TTD combines this data into detailed profiles on individual consumers that track both intimate web activity but also use highly sophisticated technology to identify a user through various separate pieces of identifying information.

133. These profiles, which include the data continuously tracked by TTD, are used as the basis for TTD's suite of products available to marketers.

B. Demand Side Platform (DSP)

134. The products TTD develops are all a part of TTD's Omnichannel Platform, which it uses to operate the largest DSP in the world.

[72] *First-Party and CRM Data*, THETRADEDESK, https://partner.thetradedesk.com/v3/portal/data/firstparty/overview (last accessed Feb. 13, 2025).

[73] *Third-Party Data Integrations*, THETRADEDESK, https://partner.thetradedesk.com/v3/portal/data/thirdparty/overview (last accessed Feb. 13, 2025).

135. An Omnichannel Platform provides "[a]dvertising that incorporates all available channels (including mobile, display, native, video, audio, and TV) into a unified strategy and ensures ads are delivered seamlessly and consistently to consumers across channels, devices, and platforms."[74]

136. TTD's DSP operates as "[t]he command and control center for creating, advertising, optimizing, and analyzing programmatic campaigns."[75] In other words, this is the platform that TTD operates to facilitate the real time bidding process.

137. Through this platform, advertisers can "[m]eet [their] audience wherever they are across digital channels and devices — including display, video, audio, digital out-of-home, and over 150 million Connected TV (CTV) households around the world."[76]

138. It comes with a "cross-device graph, [called] Identity Alliance, [that] ensures [advertisers] can reach [their] audience effectively *wherever* they're reading, watching, or listening."[77]

139. As such, TTD owns and operates "[a]n ad platform that helps advertisers buy ads through real-time bidding exchanges and manage multiple ad exchange accounts in order to optimize bidding processes using a single interface."[78]

C. KOA

140. Koa is a "[p]owerful artificial intelligence that enhances decisioning so that advertisers can extend audience reach and spend more efficiently."[79]

[74] *Glossary–Omnichannel*, *supra* note 36.

[75] *Fact Sheet*, *supra* note 29.

[76] *Demand Side Platform*, THETRADEDESK, https://www.thetradedesk.com/us/our-platform/dsp-demand-side-platform (last accessed Feb. 13, 2025).

[77] *Omnichannel Programmatic Advertising*, THETRADEDESK, https://www.thetradedesk.com/us/our-platform/omnichannel-advertising (last accessed Feb. 13, 2025) (emphasis added).

[78] *Glossary–Demand-side Platform*, *supra* note 36.

[79] *Fact Sheet*, *supra* note 29.

141. At its core Koa is “[t]he artificial intelligence that powers [the TTD] platform. Its algorithm prioritizes and selects the best-performing and most relevant inventory based on a campaign's goals, ensuring the right price is paid per impression.”[80]

142. “Koa uses a powerful predictive engine to empower advertisers with real-time recommendations and optimizations that improve campaign performance. When [an advertiser] use[s] Koa, [they]’re tapping in to [sic] the data from over 1 trillion daily queries — more than 100 times the volume of leading search engines.”[81]

143. Koa works by “analyzing robust data sets, identifying the most relevant audiences, and surfacing data-driven insights....”[82]

144. This allows advertisers to “[m]aximize performance across all channels and devices as Koa surfaces audience insights, prioritizes the most valuable impressions, and makes real-time data-driven optimizations.”[83]

145. Additionally, “Koa can process and analyze large sets of data quickly, identifying trends and opportunities to help [advertisers] choose the most relevant audiences for [an advertising] campaign.”[84]

146. Advertisers “can provide guidance and allow the AI to focus on extracting actionable insights and identifying trends. To guide and enhance Koa’s performance even further, [advertisers] can create a ‘seed’ based on ... existing knowledge about ... [their] customers. This seed serves as a reference point, enabling Koa to surface the most relevant audiences, strategies, and inventory that align with [an advertiser’s] goals and are driven by [their] first-party data.”[85]

[80] *Glossary–Koa*, *supra* note 36.

[81] *Artificial Intelligence*, THETRADEDESK, https://www.thetradedesk.com/us/our-platform/dsp-demand-side-platform/koa-ai-artificial-intelligence (last accessed Feb. 13, 2025).

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *3 Ways to Empower Koa, You AI Copilot*, THETRADEDESK (July 25, 2023), https://www.thetradedesk.com/us/resource-desk/3-ways-to-empower-koa-your-ai-co-pilot.

147. "When a client gives [TTD] their first-party data, [TTD] use[s the] seeds to build lookalike audiences that help expand reach to users with similar online behaviors to a seed audience."[86]

148. With the seed, Koa then provides advertisers with "workflow guidance to prioritize the setup and optimization decisions that will have the biggest impact on performance."[87]

149. Advertisers can even "[c]heck a real-time forecast to see how [their] changes will affect performance before you set them live."[88]

150. "Koa can help [advertisers] understand which consumers [they] should target or create a way for [advertisers] to expand [their] reach to valuable potential audiences. Koa can also evaluate consumer behavior and preferences to create similar customer profiles and segments.... It will then surface a relevance score throughout the platform so [advertisers] can easily see which of these profiles and segments are most likely to perform best based on [their] seed data."[89]

151. All in all, this combined exploitation of a consumer's data allows advertisers to maximize their profits and win the highest bid possible.[90]

D. Data Management Platform (DMP)

152. TTD's DMP allows advertisers to "[o]nboard and manage advertiser data, purchase third-party data, and customize audience models for activation."[91]

153. It "[c]ollects, processes, and stores large amounts of audience data such as cookie IDs, first-party data, and third-party data, while handling vast quantities of information in real time to better target online ads at specific audiences on a given website."[92]

[86] *Glossary–Seed*, *supra* note 36.

[87] *Programmatic Buyers*, THETRADEDESK, https://www.thetradedesk.com/us/our-platform/programmatic-buying-solutions (last accessed Feb. 13, 2025).

[88] *Id.*

[89] *Id.*

[90] *Artificial Intelligence*, *supra* note 81.

[91] *Fact Sheet*, *supra* note 29.

[92] *Glossary–Data Management Platform (DMP)*, *supra* note 36.

E. Enterprise APIs

154. "Whether jumping into real-time bidding for the first time, or looking to become more competitive in the market, The Trade Desk's APIs have everything needed to build a completely customized and scaled omnichannel bidding platform."[93]

155. As discussed above the APIs that TTD creates are "[a] set of access points and tools that enable [app] developers to build custom workflows and applications that can access certain features and data."[94]

F. Galileo

156. Galileo is customer relationship management platform, "[a] technology that stores information a company has about their customers."[95]

157. Galileo uses a technology called Unified ID 2.0 (UID2). This is "[a]n open-source ID framework that publishers, advertisers, and digital advertising platforms can use to establish the identity of a user across the open internet, while also offering users transparency and privacy controls."[96]

158. Galileo works to "connect... CRM data and deterministic IDs with a single secure identifier."[97]

159. Or in plain English, Galileo takes a company's data and uses it to create IDs connecting a particular individual to data identifying them by combining the company's data with third party data that TTD has collected.

160. This gives advertisers the ability to then match their audience across any platform they use.[98] Effectively tracking them across the internet.

[93] *Fact Sheet*, *supra* note 29.

[94] *Glossary–API*, *supra* note 36.

[95] *Glossary–Customer Relationship Management (CRM)*, *supra* note 36.

[96] *Glossary–Unified ID 2.0 (UID2)*, *supra* note 36.

[97] *Galileo*, THETRADEDESK, https://www.thetradedesk.com/us/our-platform/galileo (last accessed Feb. 17, 2025).

[98] *Id.*

III. DEFENDANT'S ADSRVR PIXEL IS PRESENT ON EACH OF THE SUBJECT WEBSITES

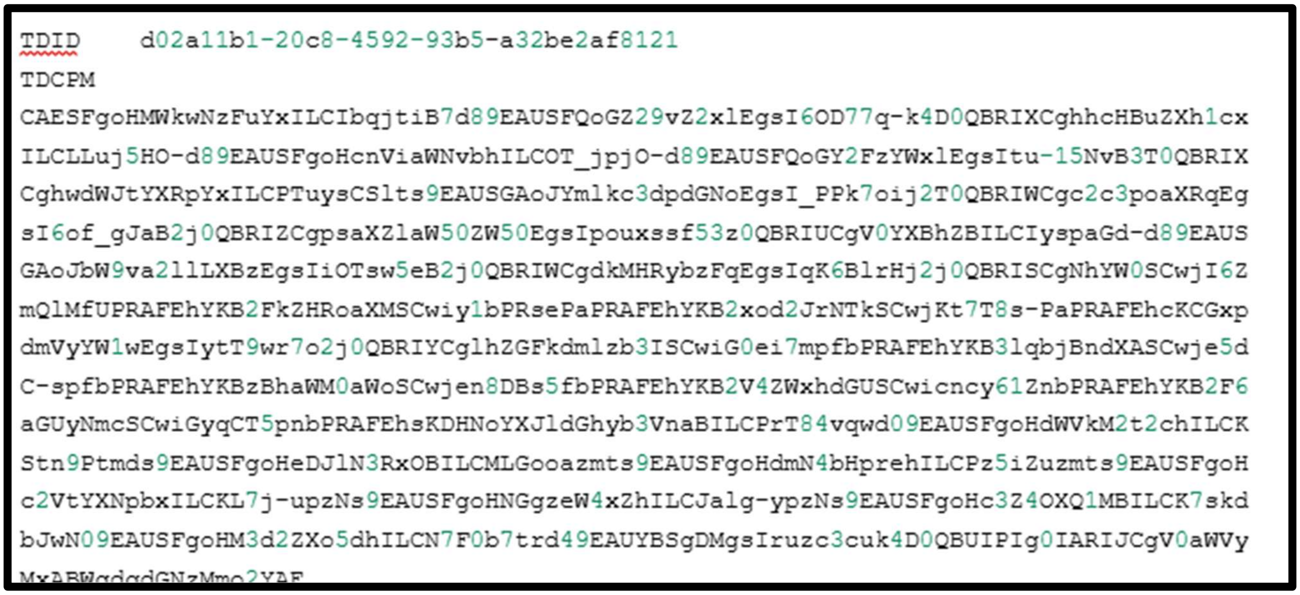
161. As demonstrated below, Defendant's Adsrvr Pixel is present on each of the websites visited by Plaintiffs, collect information on Plaintiffs' and Class Members' interactions with those websites, and assist the Pixel Partners in the wiretapping and surveillance of Plaintiffs' and Class Members on the subject websites.

A. Grubhub

162. Grubhub is a popular website where visitors can order food for delivery from restaurants in their local area.

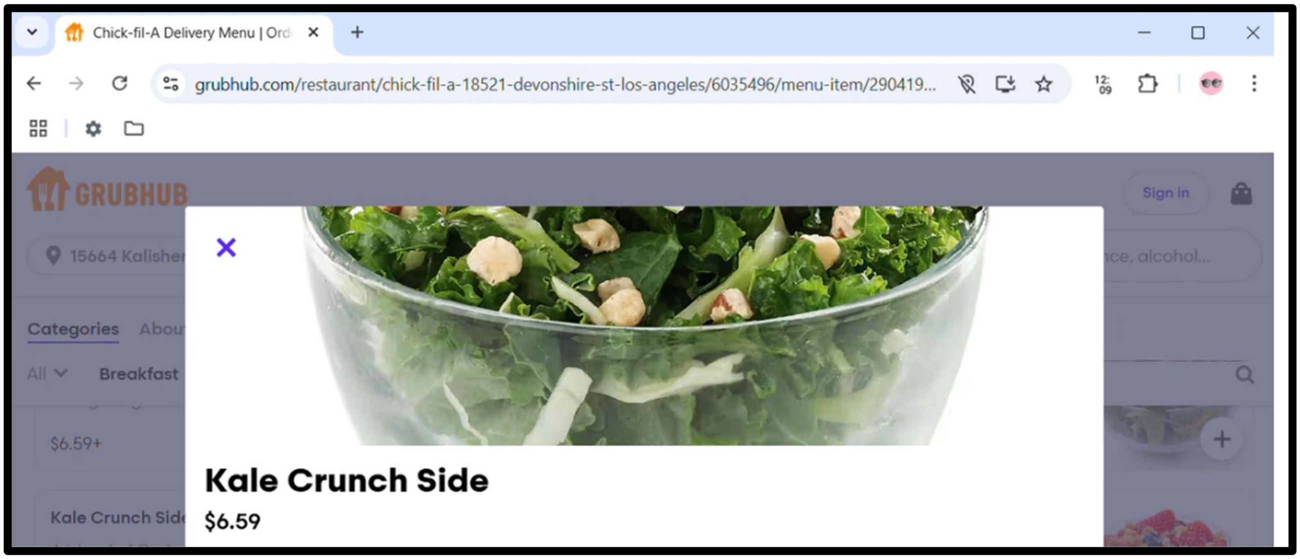
163. Unbeknownst to website visitors, the Adsrvr Pixel is loaded onto the Grubhub website.

164. As soon as a user visits the Grubhub website, the Adsrvr Pixel loads multiple cookies on that individual's browser in the manner described above.



```
TDID    d02a11b1-20c8-4592-93b5-a32be2af8121
TDCPM
CAESFgoHMWkwNzFuYxILCIbqjtiB7d89EAUSFQoGZ29vZ2xlEgsI6OD77q-k4D0QBRIXCghhcHBuZXh1cx
ILCLLuj5HO-d89EAUSFgoHcnViaWNvbhILCOT_jpjO-d89EAUSFQoGY2FzYWxlEgsItu-15NvB3T0QBRIX
CghwdWJtYXRpYxILCPTuysCSlts9EAUSGAoJYmlkc3dpdGNoEgsI_PPk7oij2T0QBRIWCgc2c3poaXRqEg
sI6of_gJaB2j0QBRIZCgpsaXZlaW50ZW50EgsIpouxssf53z0QBRIUCgV0YXBhZBILCIyspaGd-d89EAUS
GAoJbW9va2llLXBzEgsIiOTsw5eB2j0QBRIWCgdkMHRybzFqEgsIqK6BlrHj2j0QBRISCgNhYW0SCwjI6Z
mQlMfUPRAFEhYKB2FkZHRoaXMSCwiy1bPRsePaPRAFEhYKB2xod2JrNTkSCwjKt7T8s-PaPRAFEhcKCGxp
dmVyYW1wEgsIytT9wr7o2j0QBRIYCglhZGFkdmlzb3ISCwiG0ei7mpfbPRAFEhYKB3lqbjBndXASCwje5d
C-spfbPRAFEhYKBzBhaWM0aWoSCwjen8DBs5fbPRAFEhYKB2V4ZWxhdGUSCwicncy61ZnbPRAFEhYKB2F6
aGUyNmcSCwiGyqCT5pnbPRAFEhsKDHNoYXJldGhyb3VnaBILCPrT84vqwd09EAUSFgoHdWVkM2t2chILCK
Stn9Ptmds9EAUSFgoHeDJlN3RxOBILCMLGooazmts9EAUSFgoHdmN4bHprehILCPz5iZuzmts9EAUSFgoH
c2VtYXNpbxILCKL7j-upzNs9EAUSFgoHNGgzeW4xZhILCJalg-ypzNs9EAUSFgoHc3Z4OXQ1MBILCK7skd
bJwN09EAUSFgoHM3d2ZXo5dhILCN7F0b7trd49EAUYBSgDMgsIruzc3cuk4D0QBUIPIg0IARIJCgV0aWVy
MxABWqdqdGNzMmo2YAF
```

165. When a website visitor selects a restaurant and menu item for their order, that information is contained in a detailed descriptive URL.



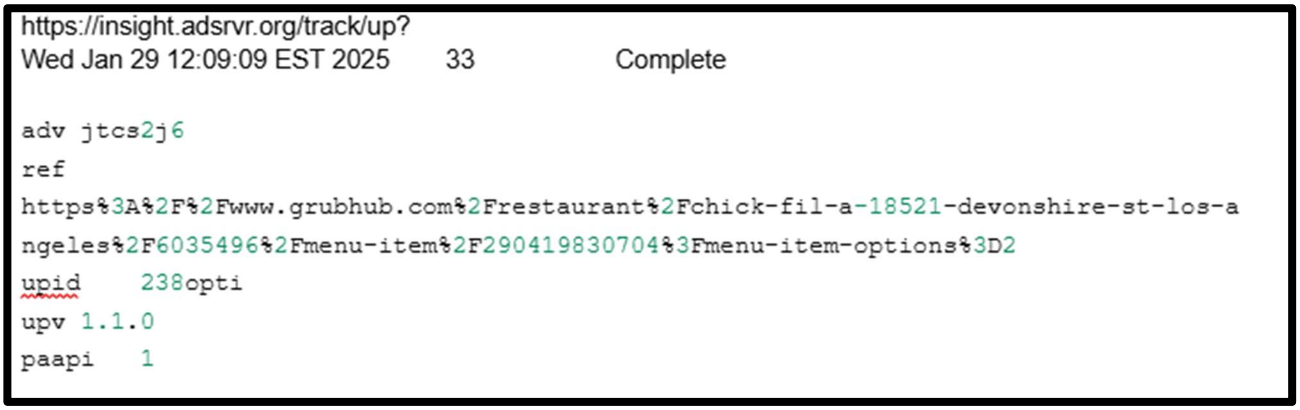
Chick-fil-A Delivery Menu | Ord

grubhub.com/restaurant/chick-fil-a-18521-devonshire-st-los-angeles/6035496/menu-item/290419...

Kale Crunch Side

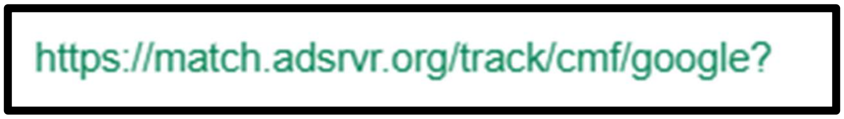
$6.59

166. As the information is entered into the website (i.e. in real time) the Adsrvr Pixel intercepts the information, including the restaurant address, name, and the unique menu item ID number, by intercepting the detailed descriptive URL.



```
https://insight.adsrvr.org/track/up?
Wed Jan 29 12:09:09 EST 2025      33              Complete

adv jtcs2j6
ref
https%3A%2F%2Fwww.grubhub.com%2Frestaurant%2Fchick-fil-a-18521-devonshire-st-los-a
ngeles%2F6035496%2Fmenu-item%2F290419830704%3Fmenu-item-options%3D2
upid    238opti
upv 1.1.0
paapi   1
```

167. The Adsrvr Pixel also provides identity resolution to Google on the Grubhub website.



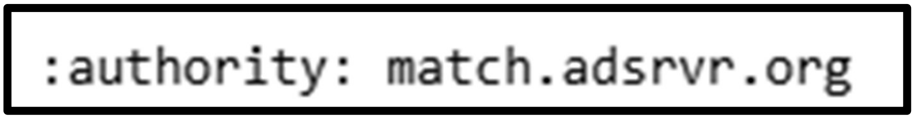
https://match.adsrvr.org/track/cmf/google?

168. 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. Buzzfeed

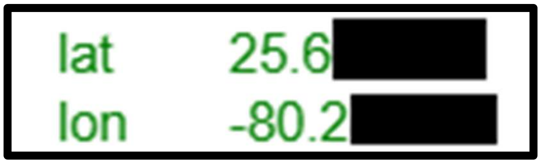
169. Buzzfeed is a popular entertainment and culture website, featuring a variety of articles and quizzes related to popular culture.

170. Unbeknownst to visitors to the Buzzfeed website, the Adsrvr Pixel is loaded onto the website.



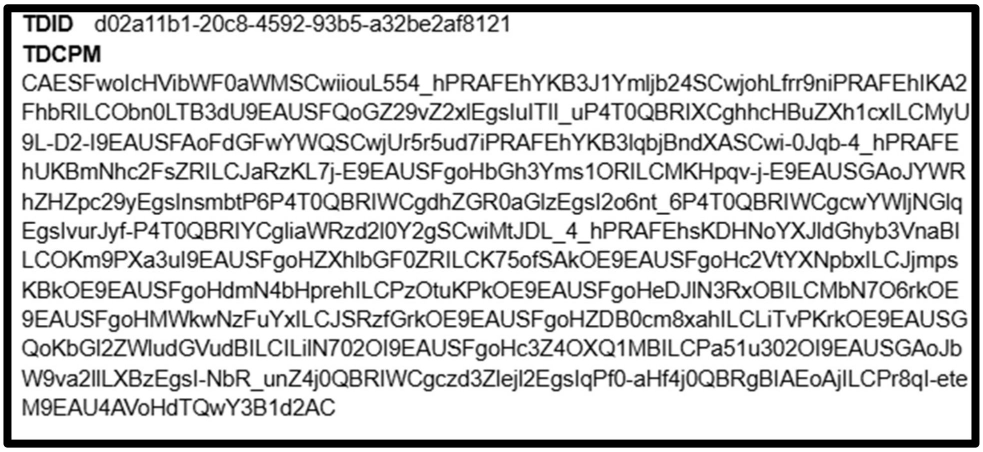
```
:authority: match.adsrvr.org
```

171. When a user visits the Buzzfeed website, the Adrvr Pixel automatically collects the user's geolocation.



```
lat     25.6[redacted]
lon     -80.2[redacted]
```

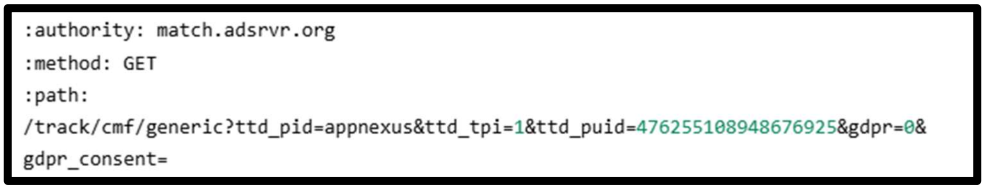
172. The Adsrvr Pixel also immediately loads the Adsrvr cookies onto the individual's browser in the manner described above.



```
TDID   d02a11b1-20c8-4592-93b5-a32be2af8121
TDCPM
CAESFwoIcHVibWF0aWMSCwiiouL554_hPRAFEhYKB3J1Ymljb24SCwjohLfrr9niPRAFEhIKA2
FhbRILCObn0LTB3dU9EAUSFQoGZ29vZ2xlEgsIuITIl_uP4T0QBRIXCghhcHBuZXh1cxILCMyU
9L-D2-I9EAUSFAoFdGFwYWQSCwjUr5r5ud7iPRAFEhYKB3lqbjBndXASCwi-0Jqb-4_hPRAFE
hUKBmNhc2FsZRILCJaRzKL7j-E9EAUSFgoHbGh3Yms1ORILCMKHpqv-j-E9EAUSGAoJYWR
hZHZpc29yEgsInsmbtP6P4T0QBRIWCgdhZGR0aGlzEgsI2o6nt_6P4T0QBRIWCgcwYWljNGlq
EgsIvurJyf-P4T0QBRIYCgliaWRzd2I0Y2gSCwiMtJDL_4_hPRAFEhsKDHNoYXJldGhyb3VnaBI
LCOKm9PXa3uI9EAUSFgoHZXhlbGF0ZRILCK75ofSAkOE9EAUSFgoHc2VtYXNpbxILCJjmps
KBkOE9EAUSFgoHdmN4bHprehILCPzOtuKPkOE9EAUSFgoHeDJlN3RxOBILCMbN7O6rkOE
9EAUSFgoHMWkwNzFuYxILCJSRzfGrkOE9EAUSFgoHZDB0cm8xahILCLiTvPKrkOE9EAUSG
QoKbGl2ZWludGVudBILCILiIN702OI9EAUSFgoHc3Z4OXQ1MBILCPa51u302OI9EAUSGAoJb
W9va2lILXBzEgsI-NbR_unZ4j0QBRIWCgczd3Zlejl2EgsIqPf0-aHf4j0QBRgBIAEoAjILCPr8qI-ete
M9EAU4AVoHdTQwY3B1d2AC
```

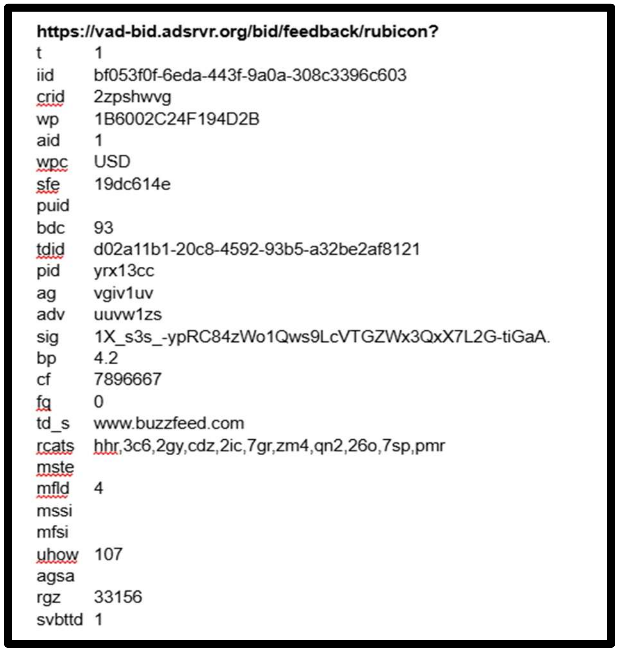
173. Defendant provides identity resolution to <u>at least 6 Partner Pixels</u> on the Buzzfeed website. Defendant is at the center of a complex web of data exchange on the Buzzfeed website.

174. With some Partner Pixels, the Adsrvr Pixel is syncing its unique ID with the ID of the Partner Pixel, which allows for each company to share the data they have collected on an individual with the other.

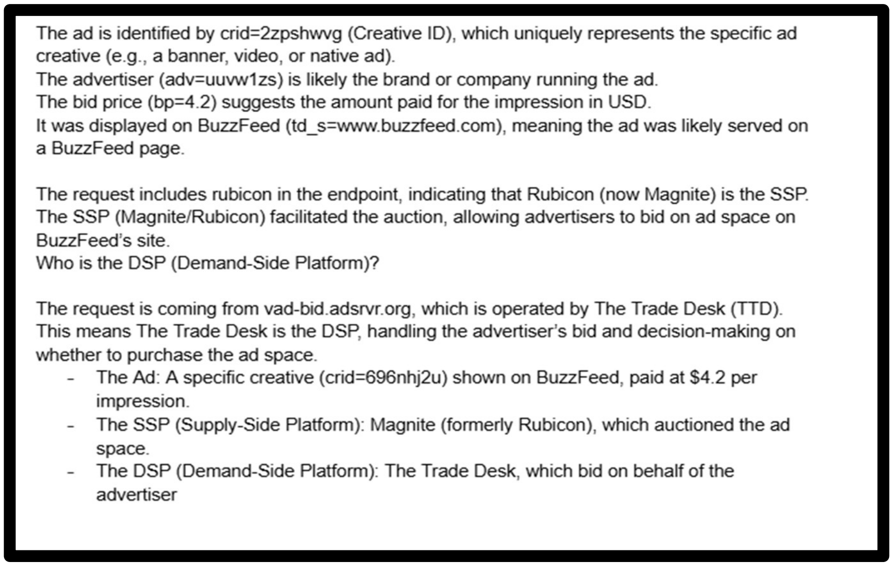


```
:authority: match.adsrvr.org
:method: GET
:path:
/track/cmf/generic?ttd_pid=appnexus&ttd_tpi=1&ttd_puid=476255108948676925&gdpr=0&
gdpr_consent=
```

175. Adsrvr also uses ID syncing to facilitate real-time bidding for advertisement on the Buzzfeed website. The image below provides an example of how the Adsrvr Pixel shares data to facilitate bidding on Adspace on the Buzzfeed website. Defendant is working with the Rubicon Pixel, a Partner Pixel, to exchange data facilitating the auction of targeted advertising to the particular website visitor.



```
https://vad-bid.adsrvr.org/bid/feedback/rubicon?
t       1
iid     bf053f0f-6eda-443f-9a0a-308c3396c603
crid    2zpshwvg
wp      1B6002C24F194D2B
aid     1
wpc     USD
sfe     19dc614e
puid
bdc     93
tdid    d02a11b1-20c8-4592-93b5-a32be2af8121
pid     yrx13cc
ag      vgiv1uv
adv     uuvw1zs
sig     1X_s3s_-ypRC84zWo1Qws9LcVTGZWx3QxX7L2G-tiGaA.
bp      4.2
cf      7896667
fq      0
td_s    www.buzzfeed.com
rcats   hhr,3c6,2gy,cdz,2ic,7gr,zm4,qn2,26o,7sp,pmr
mste
mfld    4
mssi
mfsi
uhow    107
agsa
rgz     33156
svbttd  1
```



The ad is identified by crid=2zpshwvg (Creative ID), which uniquely represents the specific ad creative (e.g., a banner, video, or native ad).
The advertiser (adv=uuvw1zs) is likely the brand or company running the ad.
The bid price (bp=4.2) suggests the amount paid for the impression in USD.
It was displayed on BuzzFeed (td_s=www.buzzfeed.com), meaning the ad was likely served on a BuzzFeed page.

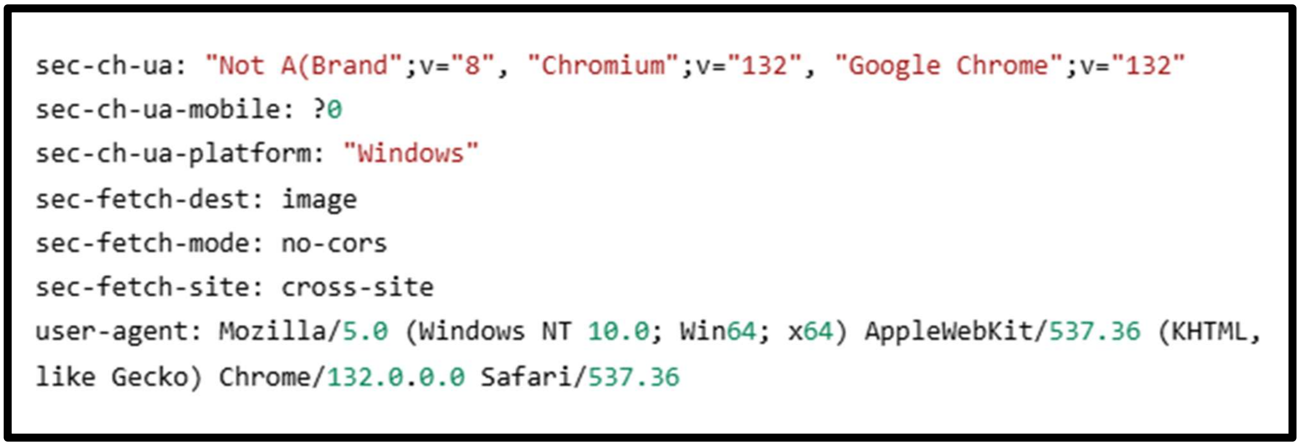
The request includes rubicon in the endpoint, indicating that Rubicon (now Magnite) is the SSP.
The SSP (Magnite/Rubicon) facilitated the auction, allowing advertisers to bid on ad space on BuzzFeed's site.
Who is the DSP (Demand-Side Platform)?

The request is coming from vad-bid.adsrvr.org, which is operated by The Trade Desk (TTD).
This means The Trade Desk is the DSP, handling the advertiser's bid and decision-making on whether to purchase the ad space.

- The Ad: A specific creative (crid=696nhj2u) shown on BuzzFeed, paid at $4.2 per impression.
- The SSP (Supply-Side Platform): Magnite (formerly Rubicon), which auctioned the ad space.
- The DSP (Demand-Side Platform): The Trade Desk, which bid on behalf of the advertiser

176. This type of ad facilitation necessarily involves 1) identifying the website visitor 2) knowing which page the individual is visiting (i.e. intercepting their selection of articles or other content and 3) sharing previously gathered information about that individual to make the advertisement more attractive to potential bidders.

177. The Adsrvr Pixel also collects device and user fingerprinting information as described above.



```
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
```

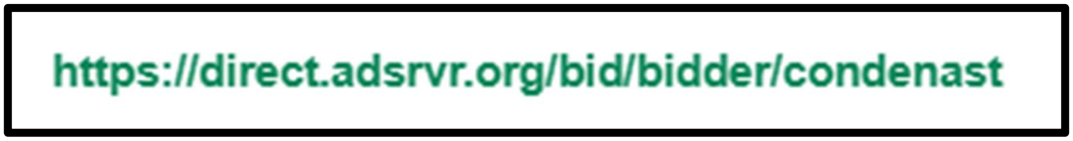
178. Defendant, because of the setting of cookies and collecting of the user's device information and IP address, tracks the future web activity of the individual and adds that information to its consumer profiles and tracking products, as well as connecting that information to users being offered up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

C. Bon Appetit

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

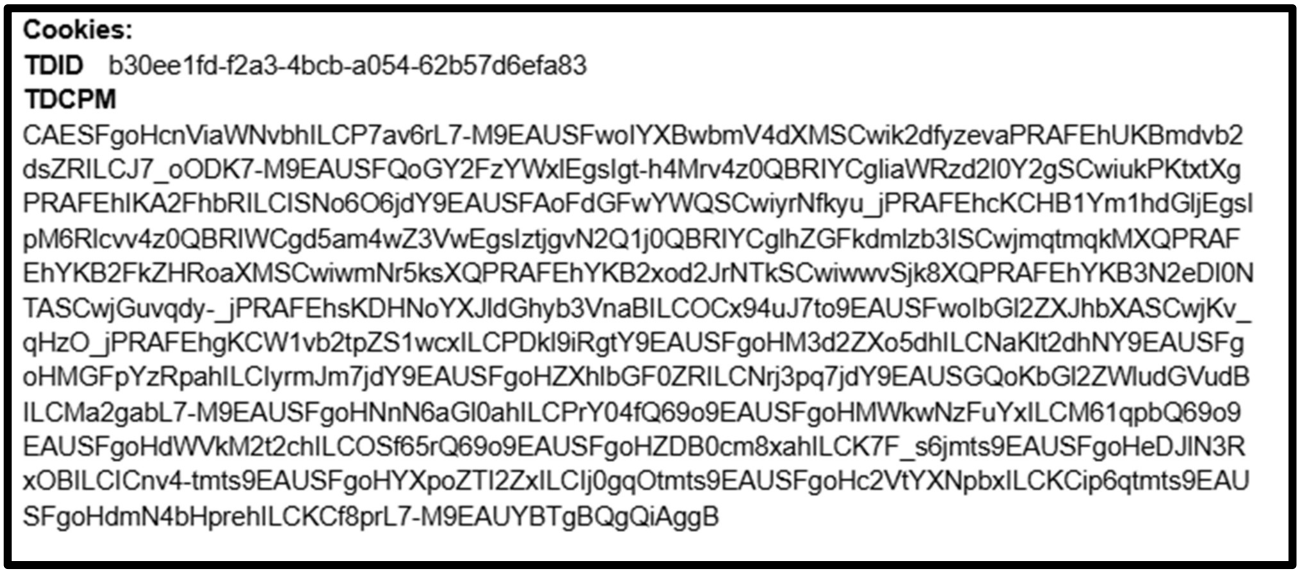
180. The website also contains ad space where companies, like Defendant, act as an advertising exchange and facilitate the real-time bidding process to hyper-target advertisements to individual website users based on data collected about their browsing activity and other activity.

181. Unbeknownst to website visitors, the Adsrvr Pixel is loaded onto the Bon Appetit website.



https://direct.adsrvr.org/bid/bidder/condenast

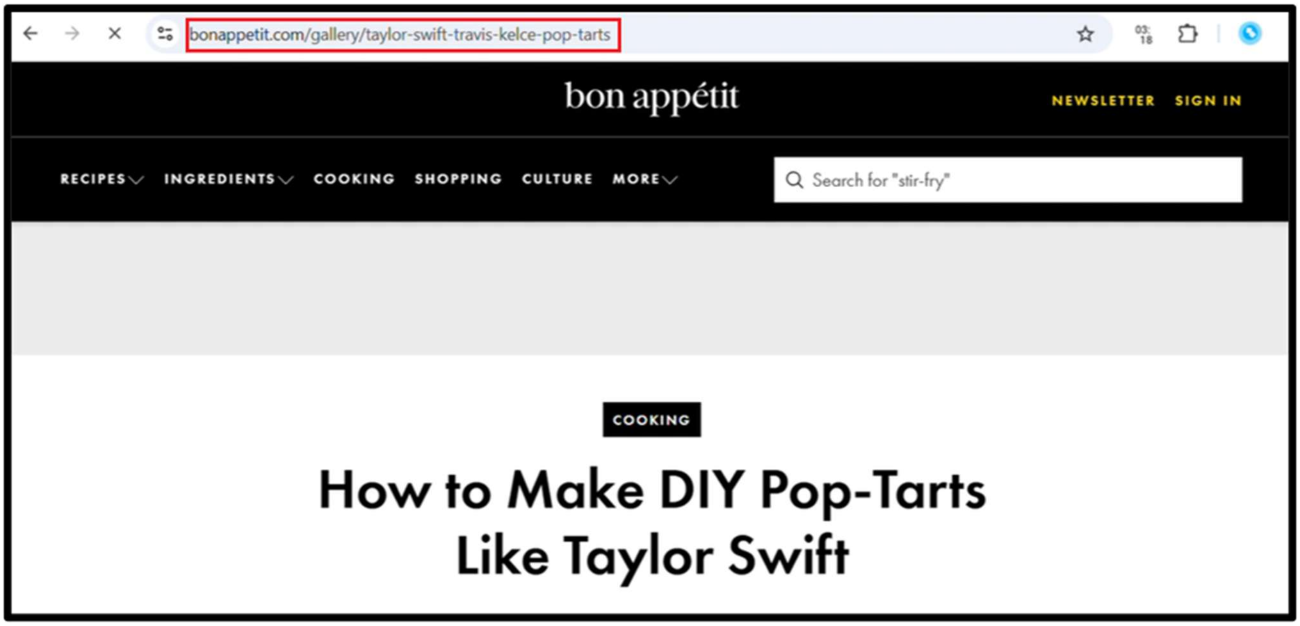
182. As soon as the individual user reaches the Bon Appetit website, the Adsrvr Pixel loads the tracking cookies onto the individual's browser in the manner described above.

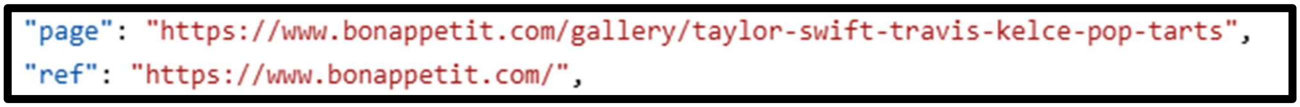


Cookies:
TDID b30ee1fd-f2a3-4bcb-a054-62b57d6efa83
TDCPM

```
CAESFgoHcnViaWNvbhILCP7av6rL7-M9EAUSFwoIYXBwbmV4dXMSCwik2dfyzevaPRAFEhUKBmdvb2
dsZRILCJ7_oODK7-M9EAUSFQoGY2FzYWxlEgsIgt-h4Mrv4z0QBRIYCgliaWRzd2l0Y2gSCwiukPKtxtXg
PRAFEhIKA2FhbRILCISNo6O6jdY9EAUSFAoFdGFwYWQSCwiyrNfkyu_jPRAFEhcKCHB1Ym1hdGljEgsI
pM6RIcvv4z0QBRIWCgd5am4wZ3VwEgsIztjgvN2Q1j0QBRIYCglhZGFkdmlzb3ISCwjmqtmqkMXQPRAF
EhYKB2FkZHRoaXMSCwiwmNr5ksXQPRAFEhYKB2xod2JrNTkSCwiwwvSjk8XQPRAFEhYKB3N2eDI0N
TASCwjGuvqdy-_jPRAFEhsKDHNoYXJldGhyb3VnaBILCOCx94uJ7to9EAUSFwoIbGl2ZXJhbXASCwjKv_
qHzO_jPRAFEhgKCW1vb2tpZS1wcxILCPDkl9iRgtY9EAUSFgoHM3d2ZXo5dhILCNaKlt2dhNY9EAUSFg
oHMGFpYzRpahILCIyrmJm7jdY9EAUSFgoHZXhlbGF0ZRILCNrj3pq7jdY9EAUSGQoKbGl2ZWludGVudB
ILCMa2gabL7-M9EAUSFgoHNnN6aGl0ahILCPrY04fQ69o9EAUSFgoHMWkwNzFuYxILCM61qpbQ69o9
EAUSFgoHdWVkM2t2chILCOSf65rQ69o9EAUSFgoHZDB0cm8xahILCK7F_s6jmts9EAUSFgoHeDJlN3R
xOBILCICnv4-tmts9EAUSFgoHYXpoZTI2ZxILCIj0gqOtmts9EAUSFgoHc2VtYXNpbxILCKCip6qtmts9EAU
SFgoHdmN4bHprehILCKCf8prL7-M9EAUYBTgBQgQiAggB
```

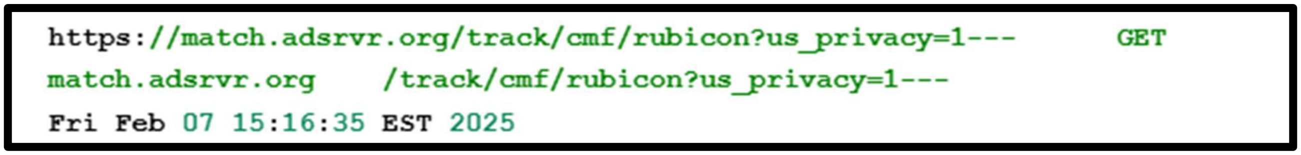
183. The Adsrvr Pixel also collects the detailed descriptive URL of the specific articles viewed by each visitor as the articles are selected on the website (i.e., in real time), and thus collects the affirmative communications of each visitor to the Bon Appetit website.


bonappetit.com/gallery/taylor-swift-travis-kelce-pop-tarts
bon appétit
NEWSLETTER
SIGN IN
RECIPES
INGREDIENTS
COOKING
SHOPPING
CULTURE
MORE
Search for "stir-fry"
COOKING
How to Make DIY Pop-Tarts Like Taylor Swift



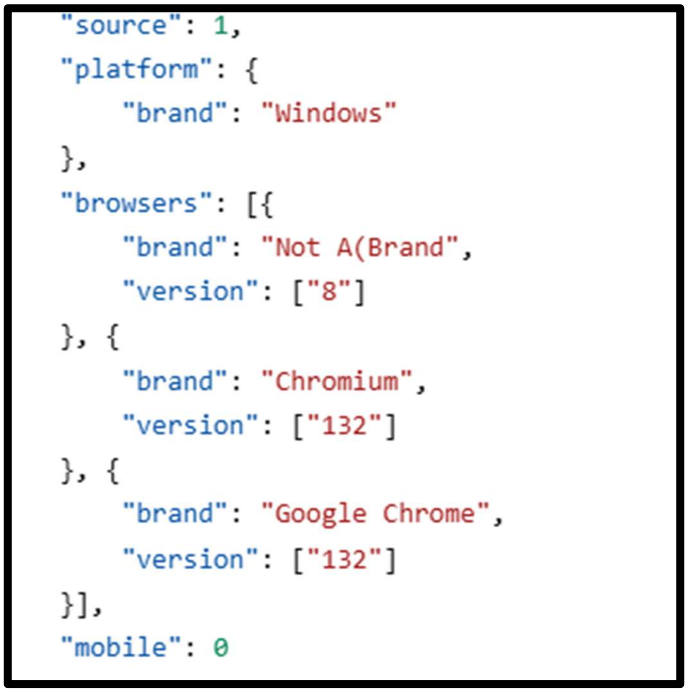
```
"page": "https://www.bonappetit.com/gallery/taylor-swift-travis-kelce-pop-tarts",
"ref": "https://www.bonappetit.com/",
```

184. Defendant, through the Adsrvr Pixel, provides identity resolution to <u>at least 22 Partner Pixels</u> on the Bon Appetite website.



```
https://match.adsrvr.org/track/cmf/rubicon?us_privacy=1---      GET
match.adsrvr.org    /track/cmf/rubicon?us_privacy=1---
Fri Feb 07 15:16:35 EST 2025
```

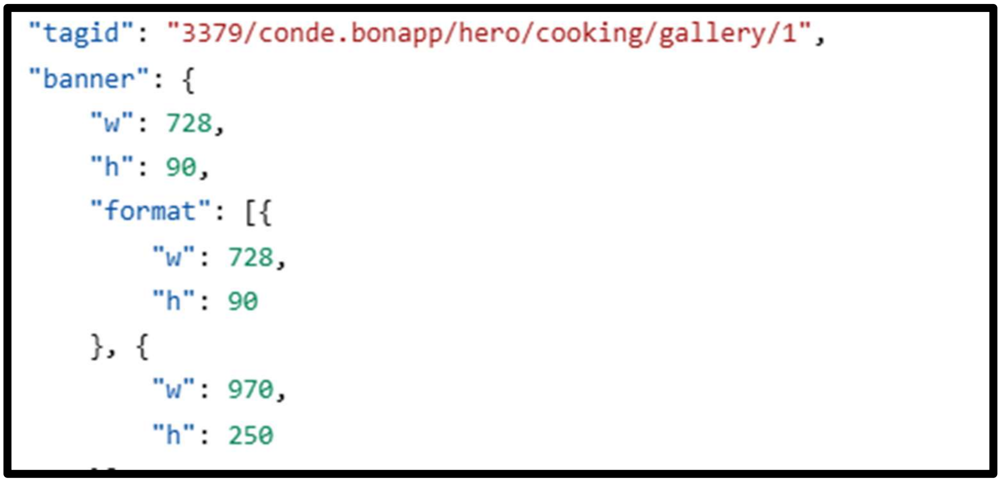
185. The Adsrvr Pixel also collects each individual's device information and digital fingerprinting as described above.



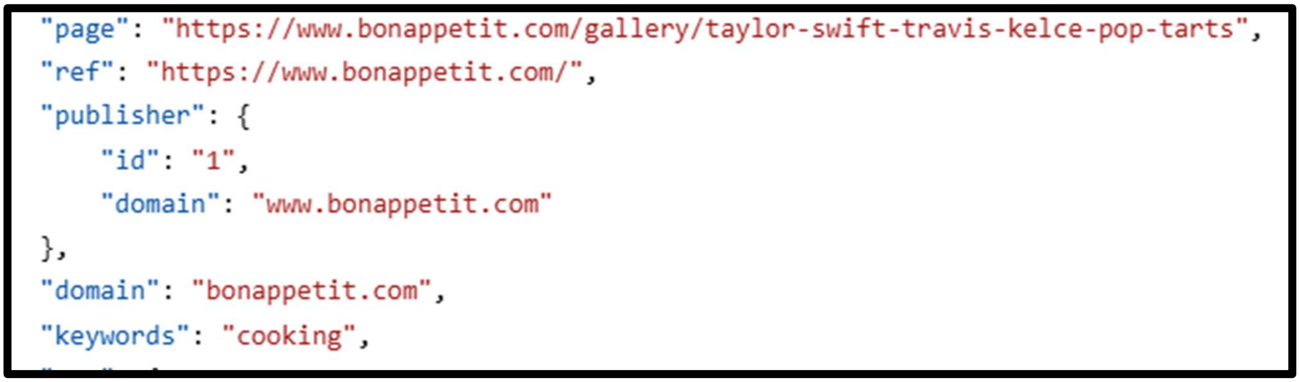
```
"source": 1,
"platform": {
    "brand": "Windows"
},
"browsers": [{
    "brand": "Not A(Brand",
    "version": ["8"]
}, {
    "brand": "Chromium",
    "version": ["132"]
}, {
    "brand": "Google Chrome",
    "version": ["132"]
}],
"mobile": 0
```

186. Defendant also services rea-time bidding for advertisements on the Bon Appetit website. To do this, Defendant shares the information it has collected on the individual website user with a number of advertisers to solicit bids for a particular ad space on the website. Plaintiffs' testing showed Defendant soliciting bids for a banner advertisement on the selected page. Lexus won the auction and paid to run the advertisement.

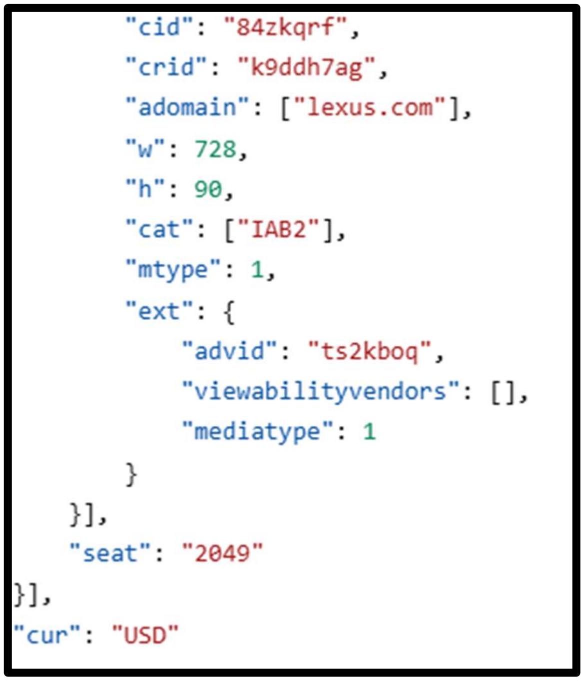
Bon Appétit's website is requesting an ad for a 728x90 banner slot on the Taylor Swift & Travis Kelce Pop-Tarts article.
The request is sent to The Trade Desk (TTD) to solicit bids from advertisers.
Lexus is seen in the response paying for their ad to be placed on the website.



```
"tagid": "3379/conde.bonapp/hero/cooking/gallery/1",
"banner": {
    "w": 728,
    "h": 90,
    "format": [{
        "w": 728,
        "h": 90
    }, {
        "w": 970,
        "h": 250
```



```
"page": "https://www.bonappetit.com/gallery/taylor-swift-travis-kelce-pop-tarts",
"ref": "https://www.bonappetit.com/",
"publisher": {
    "id": "1",
    "domain": "www.bonappetit.com"
},
"domain": "bonappetit.com",
"keywords": "cooking",
```



```
        "cid": "84zkqrf",
        "crid": "k9ddh7ag",
        "adomain": ["lexus.com"],
        "w": 728,
        "h": 90,
        "cat": ["IAB2"],
        "mtype": 1,
        "ext": {
            "advid": "ts2kboq",
            "viewabilityvendors": [],
            "mediatype": 1
        }
    }],
    "seat": "2049"
}],
"cur": "USD"
```

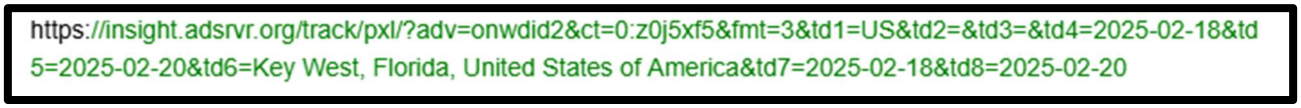
187. In addition to facilitating the technical elements of taking bids on the advertising space, awarding a winner, and servicing the ads, Defendant facilitates the sharing of the induvial website user's information to potential bidders in order to inform whether the advertisements with be sufficiently targeted to an interested individual. Using the products described above, which are created from Defendant's consumer and advertising profiles, advertisers purchase and access information previously collected by Defendant on the individual visiting the Bon Appetit website and use that information to determine whether to bid on the advertising space made available by Defendant's ad exchange.

188. 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.

D. Expedia

189. Expedia is a travel website that allows visitors to book vacations, hotels, flights, and other travel-related reservations.

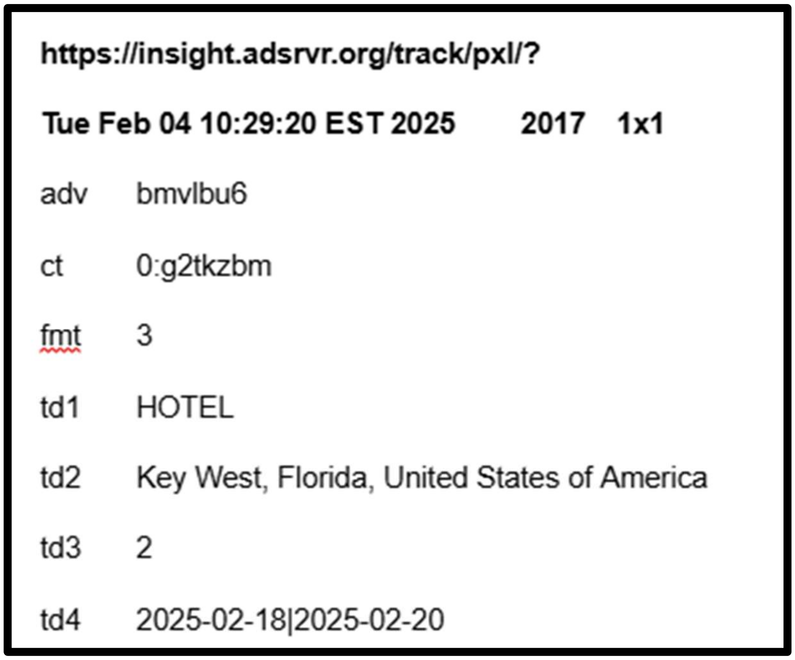
190. Unbeknownst to website visitors, the Adsrvr Pixel is loaded onto the Expedia website.



https://insight.adsrvr.org/track/pxl/?adv=onwdid2&ct=0:z0j5xf5&fmt=3&td1=US&td2=&td3=&td4=2025-02-18&td5=2025-02-20&td6=Key West, Florida, United States of America&td7=2025-02-18&td8=2025-02-20

191. When a user searches for a particular location and date—and again when they complete the purchase, the area searched and dates of booking are contained in the detailed descriptive URL of each page as described above. This process is nearly identical for every type of reservation on the Expedia website.

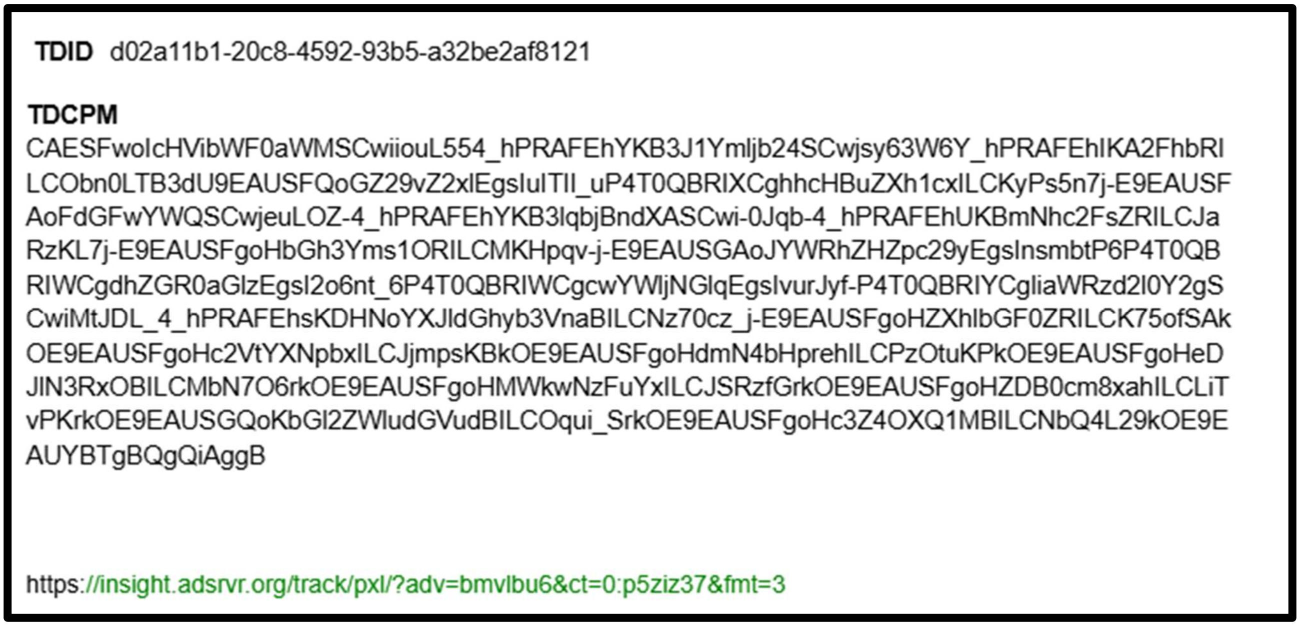
192. As that information is entered by the individual into the Expedia website (i.e., in real time) the information is intercepted by the Adsrvr Pixel.



```
https://insight.adsrvr.org/track/pxl/?

Tue Feb 04 10:29:20 EST 2025      2017    1x1

adv     bmvlbu6

ct      0:g2tkzbm

fmt     3

td1     HOTEL

td2     Key West, Florida, United States of America

td3     2

td4     2025-02-18|2025-02-20
```

193. The intercepted information is collected by Defendant, who adds it to its consumer profiles, which are included in the products described above and used in the real-time-bidding process.

194. The Adsrvr Pixel also loads multiple tracking cookies onto the browser of each visitor to the Expedia website in the manner described above.



```
TDID  d02a11b1-20c8-4592-93b5-a32be2af8121

TDCPM
CAESFwolcHVibWF0aWMSCwiiouL554_hPRAFEhYKB3J1Ymljb24SCwjsy63W6Y_hPRAFEhIKA2FhbRI
LCObn0LTB3dU9EAUSFQoGZ29vZ2xlEgsIulTIl_uP4T0QBRIXCghhcHBuZXh1cxILCKyPs5n7j-E9EAUSF
AoFdGFwYWQSCwjeuLOZ-4_hPRAFEhYKB3lqbjBndXASCwi-0Jqb-4_hPRAFEhUKBmNhc2FsZRILCJa
RzKL7j-E9EAUSFgoHbGh3Yms1ORILCMKHpqv-j-E9EAUSGAoJYWRhZHZpc29yEgsInsmbtP6P4T0QB
RIWCgdhZGR0aGlzEgsI2o6nt_6P4T0QBRIWCgcwYWljNGlqEgsIvurJyf-P4T0QBRIYCgliaWRzd2I0Y2gS
CwiMtJDL_4_hPRAFEhsKDHNoYXJldGhyb3VnaBILCNz70cz_j-E9EAUSFgoHZXhlbGF0ZRILCK75ofSAk
OE9EAUSFgoHc2VtYXNpbxILCJjmpsKBkOE9EAUSFgoHdmN4bHprehILCPzOtuKPkOE9EAUSFgoHeD
JIN3RxOBILCMbN7O6rkOE9EAUSFgoHMWkwNzFuYxILCJSRzfGrkOE9EAUSFgoHZDB0cm8xahILCLiT
vPKrkOE9EAUSGQoKbGl2ZWludGVudBILCOqui_SrkOE9EAUSFgoHc3Z4OXQ1MBILCNbQ4L29kOE9E
AUYBTgBQgQiAggB


https://insight.adsrvr.org/track/pxl/?adv=bmvlbu6&ct=0:p5ziz37&fmt=3
```

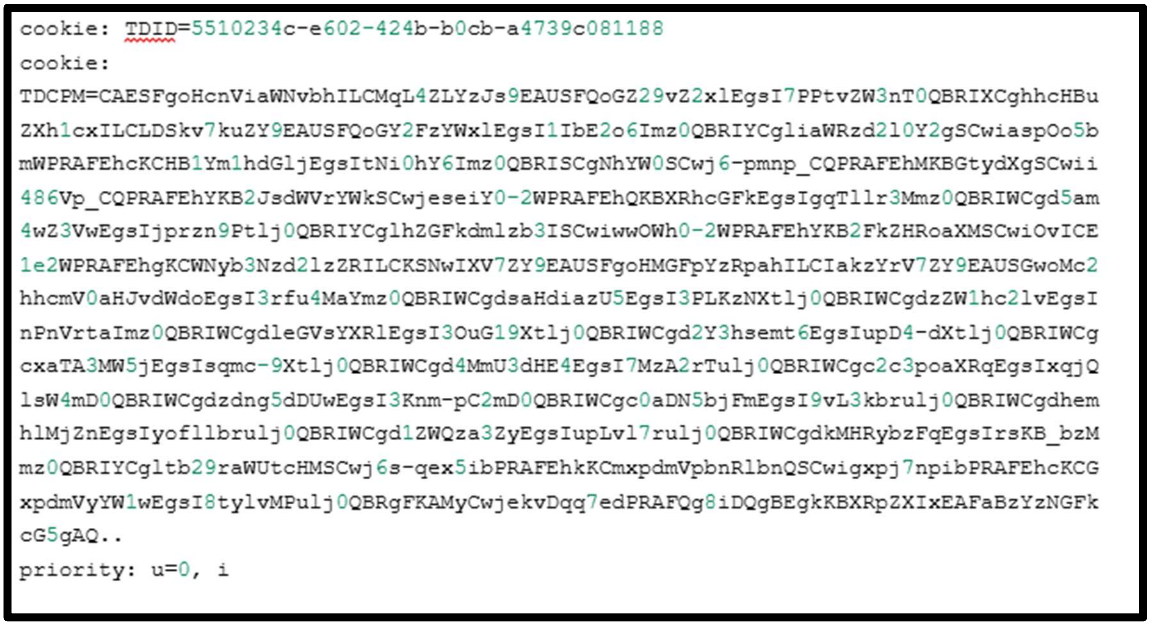
195. Defendant, because of the setting of cookies and collecting of the user's device information and IP address, tracks the future web activity of the individual and adds that information to its consumer profiles and tracking products, as well as connecting that information to users being offered up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

E. Hyatt

196. Hyatt is one of the largest hotel chains in the world. Hyatt customers can book hotel reservations on the Hyatt website.

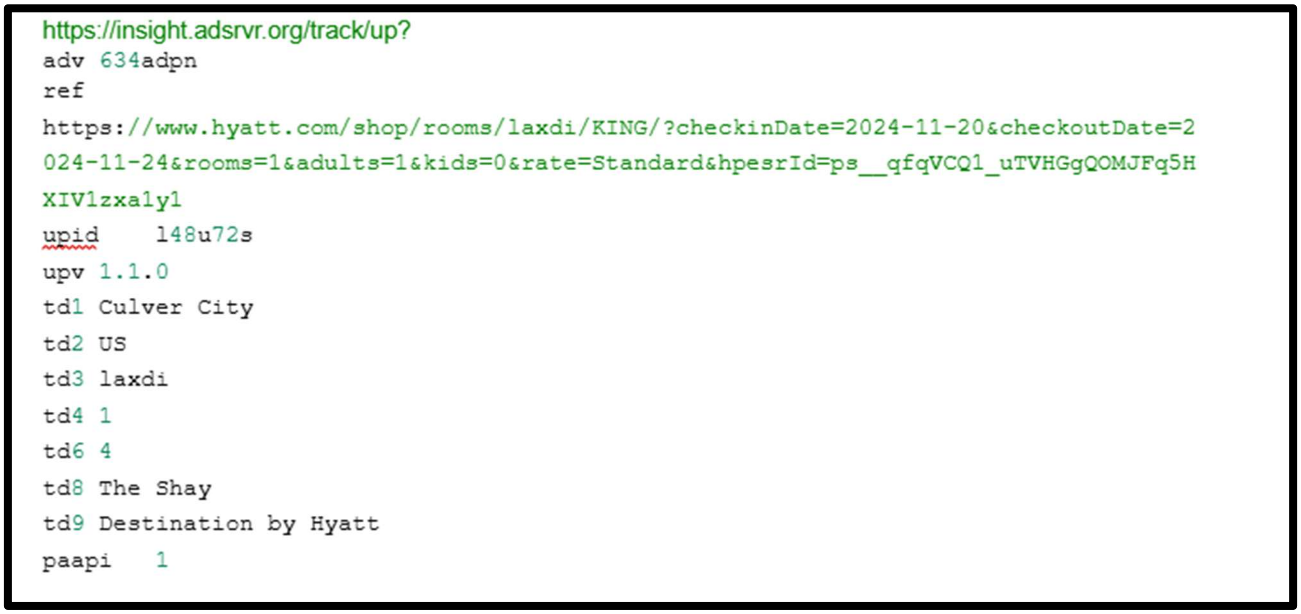
197. Unbeknownst to website visitors, the Adsrvr Pixel is loaded onto the Hyatt website.

198. The Adnxs Pixel immediately loads tracking cookies onto the individual's browser in the manner described above.



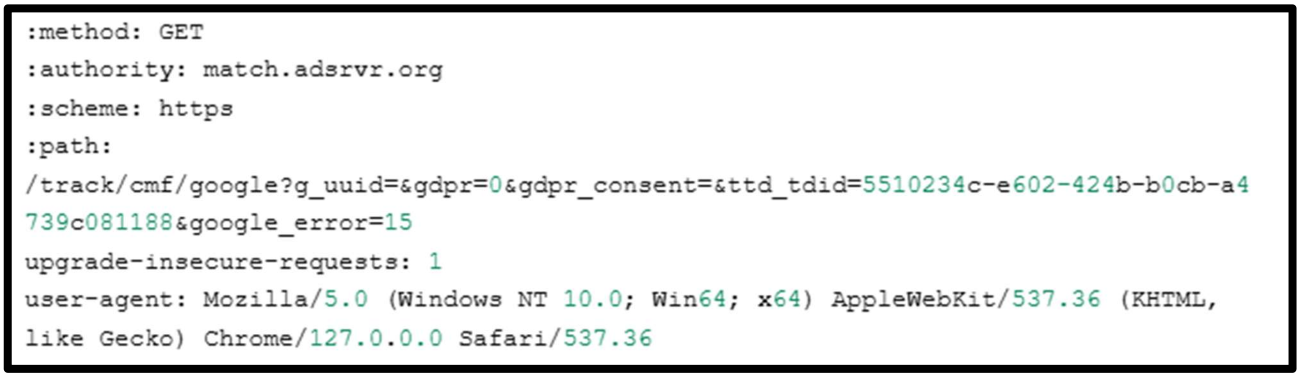
```
cookie: TDID=5510234c-e602-424b-b0cb-a4739c081188
cookie:
TDCPM=CAESFgoHcnViaWNvbhILCMqL4ZLYzJs9EAUSFQoGZ29vZ2xlEgsI7PPtvZW3nT0QBRIXCghhcHBu
ZXh1cxILCLDSkv7kuZY9EAUSFQoGY2FzYWxlEgsI1IbE2o6Imz0QBRIYCgliaWRzd2l0Y2gSCwiaspOo5b
mWPRAFEhcKCHB1Ym1hdGljEgsItNi0hY6Imz0QBRISCgNhYW0SCwj6-pmnp_CQPRAFEhMKBGtydXgSCwii
486Vp_CQPRAFEhYKB2JsdWVrYWkSCwjeseiY0-2WPRAFEhQKBXRhcGFkEgsIgqTllr3Mmz0QBRIWCgd5am
4wZ3VwEgsIjprzn9Ptlj0QBRIYCglhZGFkdmlzb3ISCwiwwOWh0-2WPRAFEhYKB2FkZHRoaXMSCwiOvICE
1e2WPRAFEhgKCWNyb3Nzd2lzZRILCKSNwIXV7ZY9EAUSFgoHMGFpYzRpahILCIakzYrV7ZY9EAUSGwoMc2
hhcmV0aHJvdWdoEgsI3rfu4MaYmz0QBRIWCgdsaHdiazU5EgsI3PLKzNXtlj0QBRIWCgdzZW1hc2lvEgsI
nPnVrtaImz0QBRIWCgdleGVsYXRlEgsI3OuG19Xtlj0QBRIWCgd2Y3hsemt6EgsIupD4-dXtlj0QBRIWCg
cxaTA3MW5jEgsIsqmc-9Xtlj0QBRIWCgd4MmU3dHE4EgsI7MzA2rTulj0QBRIWCgc2c3poaXRqEgsIxqjQ
lsW4mD0QBRIWCgdzdng5dDUwEgsI3Knm-pC2mD0QBRIWCgc0aDN5bjFmEgsI9vL3kbrulj0QBRIWCgdhem
hlMjZnEgsIyofllbrulj0QBRIWCgd1ZWQza3ZyEgsIupLvl7rulj0QBRIWCgdkMHRybzFqEgsIrsKB_bzM
mz0QBRIYCgltb29raWUtcHMSCwj6s-qex5ibPRAFEhkKCmxpdmVpbnRlbnQSCwigxpj7npibPRAFEhcKCG
xpdmVyYW1wEgsI8tylvMPulj0QBRgFKAMyCwjekvDqq7edPRAFQg8iDQgBEgkKBXRpZXIxEAFaBzYzNGFk
cG5gAQ..
priority: u=0, i
```

199. As website visitors select hotels and dates of booking (i.e. in real time), the Adsrvr Pixel intercepts this information.



```
https://insight.adsrvr.org/track/up?
adv 634adpn
ref
https://www.hyatt.com/shop/rooms/laxdi/KING/?checkinDate=2024-11-20&checkoutDate=2
024-11-24&rooms=1&adults=1&kids=0&rate=Standard&hpesrId=ps__qfqVCQ1_uTVHGgQOMJFq5H
XIV1zxa1y1
upid    148u72s
upv 1.1.0
td1 Culver City
td2 US
td3 laxdi
td4 1
td6 4
td8 The Shay
td9 Destination by Hyatt
paapi   1
```

200. Defendant also provides identity resolution to Google on the Hyatt website.



```
:method: GET
:authority: match.adsrvr.org
:scheme: https
:path:
/track/cmf/google?g_uuid=&gdpr=0&gdpr_consent=&ttd_tdid=5510234c-e602-424b-b0cb-a4
739c081188&google_error=15
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/127.0.0.0 Safari/537.36
```

201. 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.

F. Plushcare

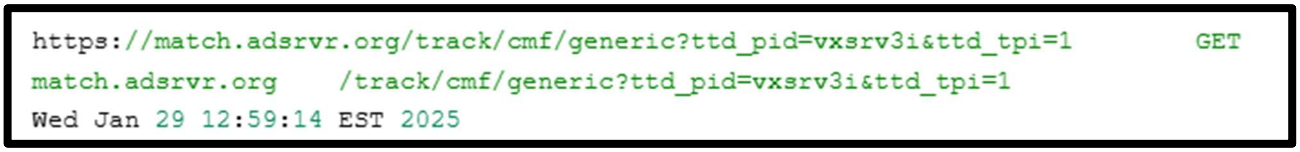
202. Plushcare is an online healthcare provider that allows its patients to make medical appointments and purchase medication on its website.

203. Unbeknownst to website visitors, the Adsrvr Pixel is loaded onto the Plushcare Website.

204. When a user visits the Plushcare website, the Adsrvr Pixel loads tracking cookies onto each individual's browser in the manner described above.

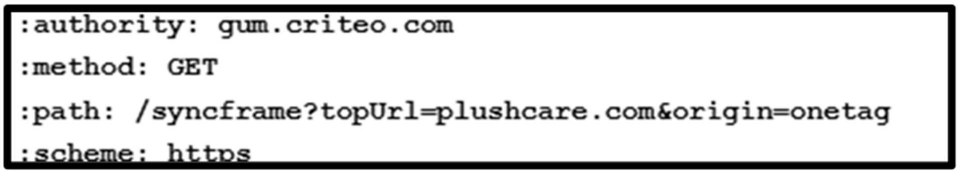
205. Defendant, because of the setting of cookies and collecting of the user's device information and IP address, tracks the future web activity of the individual and adds that information to its consumer profiles and tracking products, as well as connecting that information to users being offered up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

206. Defendant also provides identity resolution to at least 3 Partner Pixels on the Plushcare website.



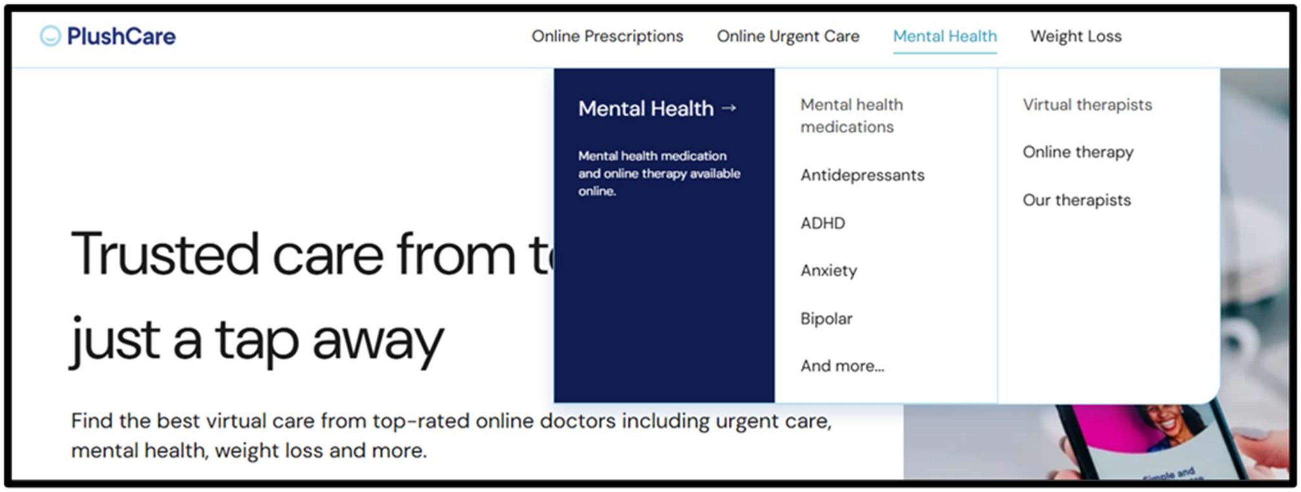
```
https://match.adsrvr.org/track/cmf/generic?ttd_pid=vxsrv3i&ttd_tpi=1        GET
match.adsrvr.org    /track/cmf/generic?ttd_pid=vxsrv3i&ttd_tpi=1
Wed Jan 29 12:59:14 EST 2025
```

207. Also unbeknownst to visitors of the Plushcare website, the Criteo Partner Pixel is loaded onto the website.



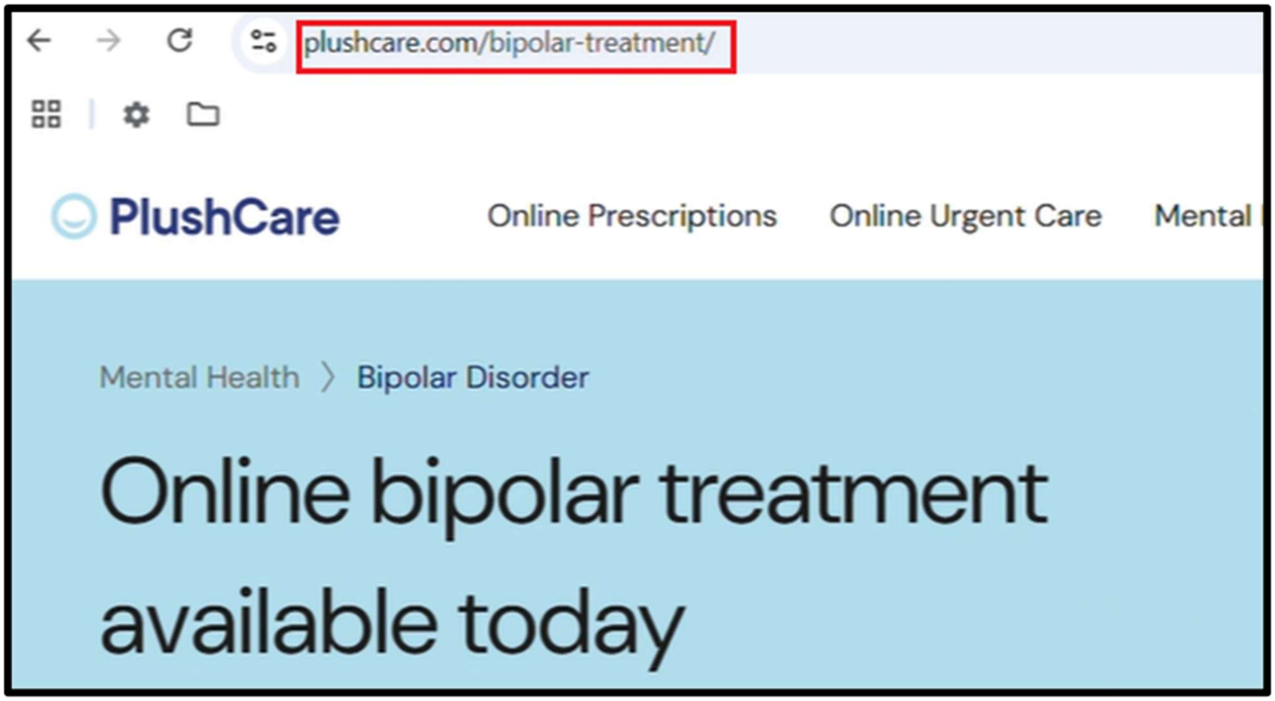
```
:authority: gum.criteo.com
:method: GET
:path: /syncframe?topUrl=plushcare.com&origin=onetag
:scheme: https
```

208. When a user selects the condition for which they are seeking treatment, that information is contained in a detailed descriptive URL as described above.



Trusted care from t
just a tap away

Find the best virtual care from top-rated online doctors including urgent care, mental health, weight loss and more.



plushcare.com/bipolar-treatment/

Mental Health 〉 Bipolar Disorder

Online bipolar treatment available today

209. As the user navigates through the website, the Criteo Pixel intercepts the URL of each page visited by each individual website visitor, thus intercepting communications between the visitor and the Plushcare website about the individual's medical symptoms and treatment.

210. The Plushcare website is the site of a large amount of data sharing by identity resolution providers. Each time these pixels interact with each other, they each exchange information with the other about the individual visiting the Plushcare website.

211. The Criteo pixel, which intercepts the information about the individual's health and treatment, then communicates with several pixels loaded onto the Plushcare website, including a pixel owned by an advertising company called Mediawallah.

212. The Mediawallah Pixel then communicates with the Adsrvr Pixel, among several other pixels.

213. As such, by way if its contract with Mediawallah, Defendant receives the intercepted health information.

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

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

214. As a result of TTD being loaded to thousands or millions of websites, Defendant is collecting various forms of PII and web activity records of millions of Americans.

215. 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.

216. Defendant also combines the data from each and every website a person visits with other data collected by the Partner Pixels to bolster the profiles TTD sells as part of its products.

217. TTD can then deanonymize the information it collects by converting sensitive PII data into actionable insights—meaning information that can be used to service hyper-targeted advertisements.

218. This is consistent with TTD's business model, which that empowers "ad buyers [to] use data-driven insights to plan, forecast [sic] and buy digital media more effectively than ever before."[99]

219. This is further evidenced by the design of TTD's products, which combine the data collected on the internet with data from other sources, a process only possible if TTD knows the identity of the person being tracked.

220. In short, the detailed profiles on nearly every aspect of every American's life require TTD to match the identity of each individual with the data collected about them. This makes the profiles much more valuable to TTD's customers and increases TTD's profits by billions of dollars.

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

221. In addition to contributing vast amounts of data to TTD's data profiles, the data collected by TTD is utilized by the Partner Pixels to conduct hyper-targeted advertising through the real-time-bidding process. *See* Factual Allegations § I.B, *supra*.

[99] *Fact Sheet*, *supra* note 29.

222. TTD's identity resolution process is a key part of a complex ecosystem of pixels which deliver detailed user information to advertisers to increase the efficiency of those advertisements.

223. When TTD shares website visitor information with a Pixel Partner, that partner (i) uses the information provided by TTD 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.

224. 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.

225. This information is provided by the Partner Pixels, who use Defendant's identity resolution 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.

226. 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.

227. 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 Jorge Hernandez-Mendoza

228. In or about February 2025, Plaintiff Hernandez-Mendoza visited the Grubhub website while in California and placed a delivery order.

229. Unbeknownst to Plaintiff Hernandez-Mendoza, the Adsrvr Pixel was loaded onto each page of the Grubhub website.

230. The Adsrvr Pixel, intercepted Plaintiff Hernandez-Mendoza's confidential communications with the Grubhub website.

231. These interceptions happened in real time as Plaintiff Hernandez-Mendoza searched for restaurants and completed his order.

232. When Plaintiff Hernandez-Mendoza visited the Grubhub website, The Adsrvr Pixel installed multiple separate cookies onto Plaintiff Hernandez-Mendoza s browser.

233. Defendant compiled the information it collected into a profile on Plaintiff Hernandez-Mendoza and added the bolstered profile to its suite of data products described above.

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

235. Plaintiff Hernandez-Mendoza 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 Hernandez-Mendoza have discovered these facts.

236. Plaintiff Hernandez-Mendoza 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.

237. Plaintiff Hernandez-Mendoza 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 Hernandez-Mendoza.

B. Plaintiff Stacy Penning

238. In or about December 2024, Plaintiff Stacy Penning visited the Buzzfeed website while in California.

239. Unbeknownst to Plaintiff Penning, the Adsrvr Pixel was loaded onto each page of the website.

240. When Plaintiff Penning visited the Buzzfeed website, The Adsrvr Pixel installed multiple separate cookies onto Plaintiff Penning's browser.

241. The Adsrvr Pixel collected information about Plaintiff Penning, including the webpages he visited and fingerprint information about his device and browser, among others.

242. Defendant shared Plaintiff Penning's unique identifiers, 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 Adsrvr Pixel.

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

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

245. Plaintiff Penning was unaware that Defendant was installing trackers on his browser, wiretapping her communications, aiding in the wiretapping of her 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 Penning have discovered these facts.

246. Plaintiff Penning 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.

247. Plaintiff Penning 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 Penning.

C. Plaintiff Laura Bonetti

248. In or about December 2024, Plaintiff Laura Bonetti visited the Bon Appetit website while in California.

249. Unbeknownst to Plaintiff Bonetti, the Adsrvr Pixel was loaded onto each page of the website.

250. When Plaintiff Bonetti visited the Bon Appetit website, The Adsrvr Pixel installed multiple separate cookies onto Plaintiff Bonetti's browser.

251. The Adsrvr Pixel collected information about Plaintiff Bonetti, including the webpages she visited and fingerprint information about her device and browser, among others.

252. Defendant shared Plaintiff Bonetti's unique identifiers, previously collected information, and information about which pages of the Bon Appetit website she visited with every Partner Pixel to which it provided identity resolution through the Adsrvr Pixel.

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

254. Defendant also shared the information it collected on Plaintiff Bonetti with advertisers to facilitate the real-time bidding process for ad space it holds on the Bon Appetit website.

255. Defendant also, by using the cookies loaded onto Plaintiff Bonetti'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.

256. Plaintiff Bonetti 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 Bonetti have discovered these facts.

257. Plaintiff Bonetti 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.

258. Plaintiff Bonetti 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 Bonetti.

D. Plaintiff Tanisha Dantignac

259. In or about August 2024, Plaintiff Tanisha Dantignac visited the Expedia website while in California and booked a flight.

260. Unbeknownst to Plaintiff Dantignac, the Adsrvr Pixel was loaded onto each page of the Expedia website.

261. The Adsrvr Pixel, intercepted Plaintiff Dantignac's confidential communications with the Expedia website, including information about her travel.

262. These interceptions happened in real time as Plaintiff Dantignac searched for flights and completed her booking.

263. When Plaintiff Dantignac visited the Expedia website, The Adsrvr Pixel installed multiple separate cookies onto Plaintiff Dantignac's browser.

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

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

266. Plaintiff Dantignac was unaware that Defendant was installing trackers on her browser, collecting his IP address, 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 Dantignac have discovered these facts.

267. Plaintiff Dantignac 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.

268. Plaintiff Dantignac 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 Dantignac.

E. Plaintiff Jessica Ju

269. In or about December 2024, Plaintiff Jessica Ju visited the Hyatt website while in California and made a hotel reservation.

270. Unbeknownst to Plaintiff Ju, the Adsrvr Pixel was loaded onto the Hyatt website.

271. When Plaintiff Ju visited the Hyatt website, The Adsrvr Pixel installed multiple separate cookies onto Plaintiff Ju's browser.

272. As Plaintiff Ju selected her hotel and dates of stay and made her purchase (i.e. in real time), the Adsrvr Pixel intercepted that information.

273. The Adsrvr Pixel then shared the information about Plaintiff Ju's reservation with Partner Pixels loaded on the Hyatt website.

274. The Adsrvr Pixel also collected information about Plaintiff Ju, including the webpages she visited and fingerprint information about her device and browser, among others.

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

276. Defendant also shared the information it collected on Plaintiff Ju with advertisers to facilitate the real-time bidding process as described above.

277. Defendant also, by using the cookies loaded onto Plaintiff Ju'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.

278. Plaintiff Ju 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 Ju have discovered these facts.

279. Plaintiff Ju 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.

280. Plaintiff Ju 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 Ju.

F. Plaintiff Robert Mason

281. In or about February 2021, Plaintiff Robert Mason visited the Plushcare website while in California and made a medical appointment.

282. Unbeknownst to Plaintiff Mason, the Criteo Pixel was loaded onto each page of the Plushcare website.

283. The Criteo Pixel, by receiving the detailed URL of each page of the website, intercepted Plaintiff Mason's confidential communications with the Plushcare website, including information about his medical condition and treatment.

284. Unbeknownst to Plaintiff Mason, the Adsrvr Pixel was loaded onto each page of the Plushcare website.

285. These interceptions happened in real time as Plaintiff Mason entered confidential information on the website.

286. Defendant contracted with Mediawallah and, by extension, Criteo to receive intercepted information about Plaintiff Mason, aiding Criteo's wiretapping.

287. When Plaintiff Mason visited the Plushcare website, The Adsrvr Pixel installed multiple separate cookies onto Plaintiff Mason's browser.

288. The Adsrvr Pixel collected information about Plaintiff Mason, including the webpages he visited and fingerprint information about his device and browser, among others.

289. Defendant shared Plaintiff Mason's unique identifiers, previously collected information, and information about which pages of the Plushcare website he visited with every Partner Pixel to which it provided identity resolution through the Adsrvr Pixel.

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

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

292. Plaintiff Mason was unaware that Defendant was installing trackers on his browser, collecting his IP address, wiretapping her 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 Mason have discovered these facts.

293. Plaintiff Mason 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.

294. Plaintiff Mason 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 Mason.

CLASS ACTION ALLEGATIONS

295. **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 made available for sale or use through Defendant's products or partnerships.

296. **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 made available for sale or use through Defendant's products or partnerships.

297. 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.

298. Excluded from the Classes are Defendant, any affiliate, parent, or subsidiary of 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.

299. **Numerosity**. Members of the Classes 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.

300. **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.

301. **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.

302. **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 wasw 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 ECPA, CIPA or any other relevant statute;

303. **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

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

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

306. Plaintiffs bring this claim pursuant to California law.

307. 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).

308. 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.

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

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

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

312. 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 its products.

(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 disclose 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.

313. 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.

314. 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.

315. 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)

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

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

318. 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.

319. 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.").

320. 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).

321. 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.

322. 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.

323. Defendant's Adsrvr Pixel and SDKs are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

324. 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).

325. 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 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.

326. 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.

327. 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.

328. The wiretapping of Plaintiffs and California Subclass Members occurred in California, where Plaintiffs and California Subclass Members accessed the websites, where Defendant's ADSRVR pixel was loaded on Plaintiffs' and California Subclass Members' browsers, and where Defendant routed Plaintiffs' and California Subclass Members' electronic communications to Defendant's servers.

329. Further, Defendant aided, agreed with, employed and/or conspired with an unknown number of Partner Pixels to facilitate the Partner Pixels' wiretapping of Class Members' communications by providing identity resolution to those Partner Pixels.

330. 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 seek statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

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

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

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

333. 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."

334. 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).

335. 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).

336. 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.

337. 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.

338. 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 the Defendants' 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").

339. The Adsrvr Pixel and the cookies TTD installed on Plaintiffs' and California Subclass Members' browsers, to the extent they do not intercept "contents" of communications as defined in CIPA § 631(a), are "pen registers" because they are "device[s] or process[es]" that "capture" 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.

340. At all relevant times, Defendant installed the Adsrvr Pixel and cookies—which are pen registers—on Plaintiffs' and California Subclass Members' browsers, which enabled Defendant to collect Plaintiff's and California Subclass Members' IP addresses, geolocation, device information, and other persistent identifiers from the websites they visited. Defendant then used the Adsrvr Pixel and cookies 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.

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

342. Defendant did not obtain a court order to install or use the Adsrvr Pixel, cookies, and other tracking technology at issue.

343. 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

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

345. Plaintiffs bring this claim individually and on behalf of the Classes against Defendant pursuant to California law.

346. 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.

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

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

349. 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.

350. 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.

351. 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.

352. Defendant was aware of the benefit conferred by Plaintiffs. Indeed, Defendant's 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.

<u>COUNT V</u>
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1), *et seq*

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

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

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

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

357. 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.

358. 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).

359. 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).

360. 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).

361. 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).

362. 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).

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

(a) The Adsrvr Pixel;

(b) Any other tracking code or SDK used by Defendant;

(c) Each Partner Pixel;

364. Plaintiffs' and Class Members' interactions with each website are electronic communications under the ECPA.

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

366. Defendant intercepted communications that include, but are not limited to, communications to/from Plaintiffs 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.

367. 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).

368. 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.

369. 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).

370. Defendant was not acting under the color of law to intercept Plaintiff' and Class Members' wire or electronic communications.

371. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy. Plaintiffs 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.

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

373. 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, individually and on behalf of all others similarly situated, seeks 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 DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: March 28, 2025

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
E-mail: 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 Plaintiff