UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STACY PENNING, SUNGGIL HONG, LAURA BONETTI, JONATHAN FINESTONE, TANISHA DANTIGNAC, and ROBERT MASON, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

MICROSOFT CORPORATION,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

PAGE

Plaintiffs Stacy Penning, SungGil Hong, Laura Bonetti, Jonathan Finestone, Tanisha Dantignac, and Robert Mason ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Microsoft Corporation ("Microsoft" or "Defendant"). Plaintiffs bring this action based upon personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

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

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

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

THE PARTIES

I. PLAINTIFFS

4. ***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 he accessed the Buzzfeed website and had his activity on that website and subsequent activity on other websites tracked by Defendant.

5. ***Plaintiff SungGil Hong***. Plaintiff SungGil Hong is a natural person and citizen of California, residing in San Diego, California. Plaintiff Hong was in California when he accessed the AliExpress website and had his 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 Jonathan Finestone.*** Plaintiff Jonathan Finestone is a natural person and citizen of California, residing in West Hollywood, California. Plaintiff Finestone was in California when he accessed the Hyatt website and had his activity on that website and subsequent activity on other websites tracked by Defendant.

8. ***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.

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.

II. DEFENDANT

10. Defendant Microsoft Corporation is a Washington corporation with its principal place of business in Redmond, Washington. Microsoft uses its proprietary technology, including but not limited to the Adnxs Pixel and Xandr platform to accomplish the widespread surveillance and unlawful sharing and sale of data alleged herein.

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 at least one Defendant.

12. This Court has personal jurisdiction over Defendant because Defendant is headquartered and incorporated in Washington.

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

FACTUAL ALLEGATIONS

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

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]

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,"

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

[2] Sherman, *supra*, 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: PROCEEDINGS OF THE 2015 ACM ON CONFERENCE ON ONLINE SOCIAL NETWORKS 71, 71 (2015), https://dl.acm.org/doi/pdf/10.1145/2817946.2817957.

such as websites visited.[4] Inferred data "is gleaned from observed data by modelling or profiling," meaning what consumers may be *expected* to do.[5] 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."[6]

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."[7] 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."[8]

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."[9]

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*, at 11, NATO Strategic Communications Centre Of Excellence, (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[5] *Id.*

[6] *Id.*

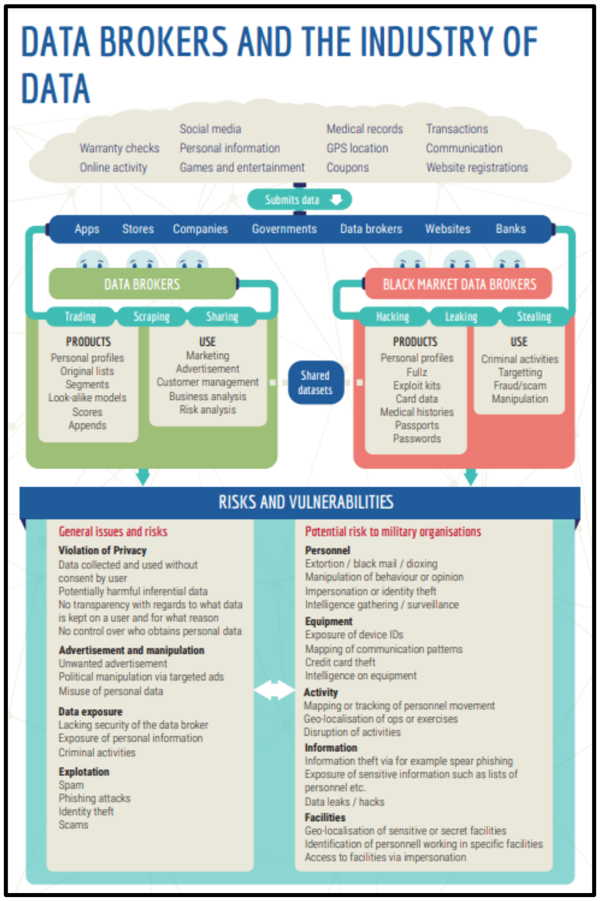
[7] Sherman, *supra*, at 1.

[8] *Id.*

[9] *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. 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.[10]

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.[11]



General issues and risks

Violation of Privacy
Data collected and used without consent by user
Potentially harmful inferential data
No transparency with regards to what data is kept on a user and for what reason
No control over who obtains personal data

Advertisement and manipulation
Unwanted advertisement
Political manipulation via targeted ads
Misuse of personal data

Data exposure
Lacking security of the data broker
Exposure of personal information
Criminal activities

Explotation
Spam
Phishing attacks
Identity theft
Scams

Potential risk to military organisations

Personnel
Extortion / black mail / dioxing
Manipulation of behaviour or opinion
Impersonation or identity theft
Intelligence gathering / surveillance

Equipment
Exposure of device IDs
Mapping of communication patterns
Credit card theft
Intelligence on equipment

Activity
Mapping or tracking of personnel movement
Geo-localisation of ops or exercises
Disruption of activities

Information
Information theft via for example spear phishing
Exposure of sensitive information such as lists of personnel etc.
Data leaks / hacks

Facilities
Geo-localisation of sensitive or secret facilities
Identification of personnell working in specific facilities
Access to facilities via impersonation

[10] *Id.*

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

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 like Defendant to track users across the Internet.[12]

23. 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."[13]

24. 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.[14]

25. 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.

B. Real-Time Bidding

26. So, 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—and the Microsoft software that is at issue in this action—comes in.

27. "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."[15]

[12] *Id.* at 11.

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

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

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

28. "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] with website or app publishers to help them participate in the RTB process." "DSPs primarily work with advertisers to help them evaluate the value of user impressions and optimize the bid prices they put forth."[16] 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."[17]

29. In other words, (i) SSPs work with website operators to provide user information to advertisers that might be interested in those users; (ii) DSPs work with advertisers to help advertisers select which users to target, and ultimately make bid to show advertisements to selected users; and (iii) an Advertising Exchange is the platform on which all of this happens.

30. As described in more detail below, Microsoft participates on all sides of this process. The Adnxs Pixel—now known as "Microsoft Invest"—is a DSP,[18] and Xandr provides both an SSP and DSP.[19] This tracks with the trend of many technology companies serving both the "publisher" and "advertiser" (supply and demand, respectively) sides of the RTB ecosystem.[20]

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.

[16] Geoghegan, *supra*.

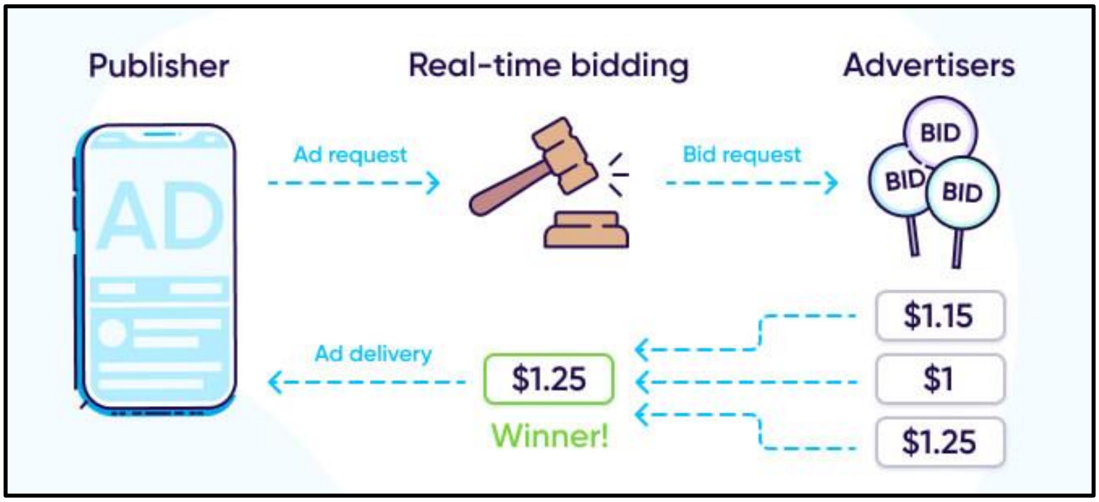
[17] *Introducing To Ad Serving*, MICROSOFT IGNITE (Mar. 3, 2024), https://learn.microsoft.com/en-us/xandr/industry-reference/introduction-to-ad-serving.

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

[19] *Introducing To Ad Serving*, *supra*.

[20] *See* Amir Sharer, *Why SSPs and DSPs are Breaking the Barrier Between Supply and Demand*, ADEXCHANGER (May 2, 2024), https://www.adexchanger.com/data-driven-thinking/why-ssps-and-dsps-are-breaking-the-barrier-between-supply-and-demand/.

> 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.[21]

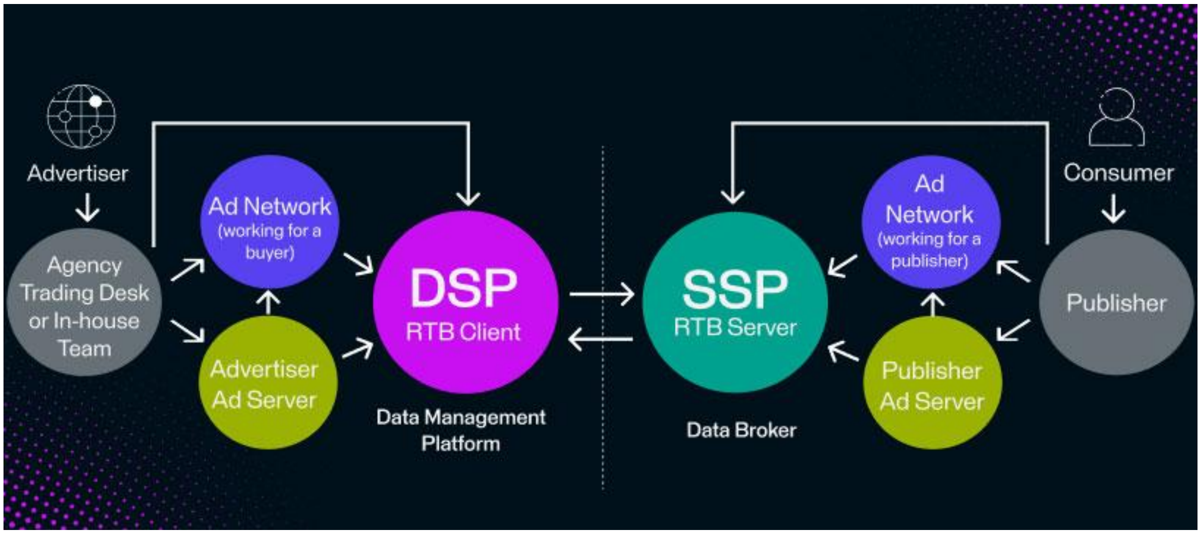


32. Facilitating this real-time bidding process means SSPs and DSPs—like those offered by Microsoft—must have as much information as possible about consumers to procure the greatest interest from advertisers and obtain the highest bids for website and app operators' users. But these SSPs and DSPs receive assistance by connecting with other third parties like data brokers and Data Management Platforms ("DMPs") to de-anonymize users and bolster the information they can either provide to advertisers or advertisers can consider when making bids:

> the economic incentives of an auction mean that DSP with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The DSP enlists a final actor, the data management platform (DMP) [or data broker, like 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.[22]

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

[22] 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*



33. In other words, before bidding to show a user an advertisement, SSPs and DSPs like those offered by Defendant will attempt to determine what other information about a user may be available. SSPs and DSPs do this by connecting with entities like data brokers, DMPs, and the like, who match a consumer's information from a particular website or mobile application (*e.g.*, their IP address, device metadata, other unique identifiers) with any profiles on those users data brokers 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. 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,

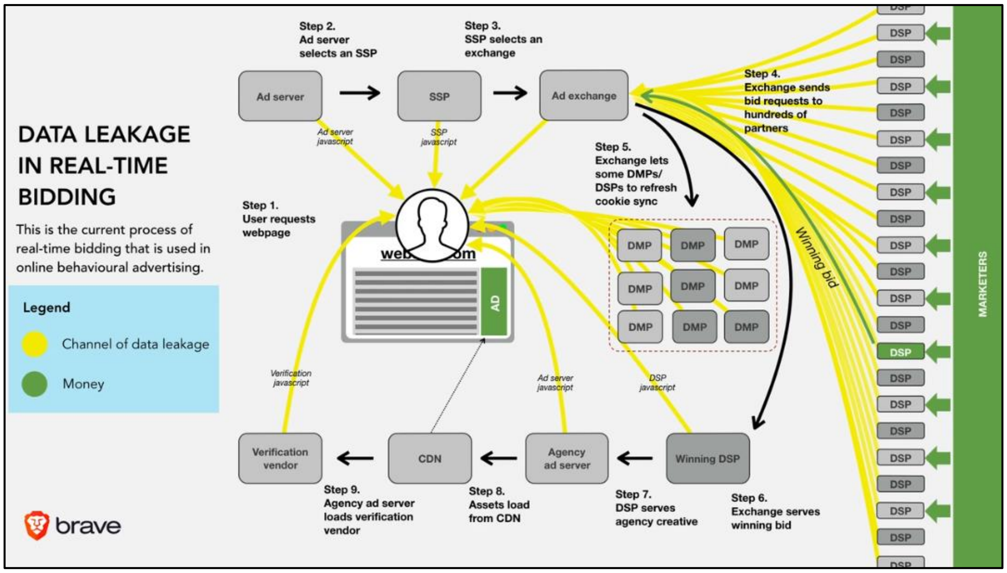
PERION, WHAT IS A SUPPLY-SIDE PLATFORM (SSP): DEFINITION AND IMPORTANCE, https://perion.com/publishers/what-is-a-supply-side-platform-ssp-definition-and-importance/.

> 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."[23]

35. The last point bears additional emphasis, as it means the data Defendant provides through its DSP services 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.

36. 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."[24]

37. For these reasons, some have characterized "real-time bidding" as "[t]he biggest data breach ever recorded" because of the sheer number of entities that receive personal information[25]:


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

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

[24] Geoghegan, *supra*.

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

38. 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

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

40. 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."[26] This allows entities like Defendant to circumvent "the restriction that sites can't read each other cookies, in order to better facilitate targeting and real-time bidding."[27]

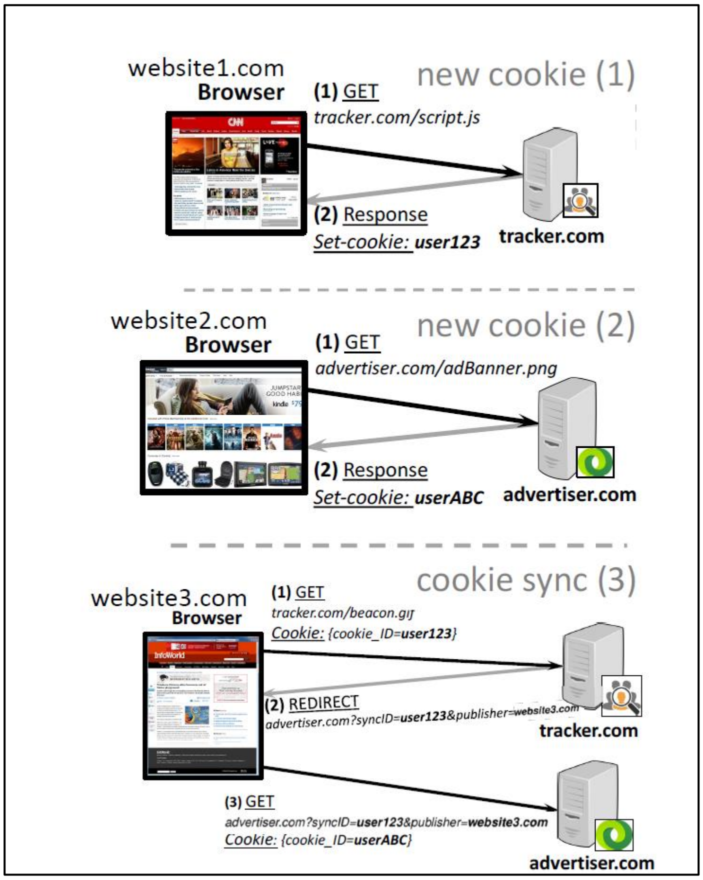
41. Cookie syncing works as follows:

> 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.

[26] 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.

[27] 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)

> 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.*[28]



42. 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

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

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.[29]

43. On the flip side, "CSync may re-identify web users even after they delete their cookies."[30] "[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."[31] 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."[32]

44. Thus, "syncing userIDs of a given user increases the user identifiability while browsing, thus reducing their overall anonymity on the Web."[33]

45. Cookie syncing is precisely what is happening here. When Defendant's technology like the Adnxs Pixel is installed on users' browsers, Defendant's technology syncs Defendant's 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.

* * *

46. To summarize the proceeding allegations, data brokers focus on collecting as much information about users as possible to create comprehensive user profiles. Through "cookie syncing," those profiles are shared with Defendant's advertising technologies and other entities (and vice versa) to form the most fulsome picture (literally, a profile) with the most attributes as possible.

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

[30] *Id.*

[31] *See id.*

[32] *Id.*

[33] *Id.* at 1441.

And those profiles and sold to and bought by advertisers through real-time bidding using the technology Defendant implements on the websites, 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.

47. Accordingly, Defendant is using its conjunction in conjunction with website operators and other third parties to (i) de-anonymize users, (ii) allow users to be bought by and sold to advertisers in real-time bidding, and (iii) allow website operators to monetize websites by installing Defendant's Pixels and allowing Defendant to collect as much information about users as possible (without consent).

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

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

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

A. Adnxs Pixel

50. Microsoft oversees a massive web of online tracking technologies that provide ongoing information to Microsoft and its partners.

49. The collection of this highly detailed information relies on a series of "pixels" loaded onto websites.

50. A pixel is a piece of code that website operators can integrate into their websites to "track[] the people and type of action they take."[34]

[34] *Retargeting*, Meta, https://www.facebook.com/business/goals/retargeting (last accessed Feb. 12, 2025).

51. Microsoft collects information on Internet users' activity on a wide variety of websites using the Adnxs Pixel, a pixel it owns and develops and through partnering with other data brokers and advertisers.

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

53. Plaintiffs' testing revealed that the Adnxs Pixel interacts with dozens of Partner Pixels on websites across the internet.

54. Microsoft collects additional data from Internet users through Microsoft's interactions with users and through Microsoft's products.[35] Microsoft collects data by and through users' interactions, use, and experiences with Microsoft's products.[36] Microsoft also obtains data about Internet users from Microsoft affiliates, subsidiaries, and third parties.[37] Microsoft shares data "with Microsoft-controlled affiliates and subsidiaries [and] with vendors working on [Microsoft's] behalf."[38] This data is combined with the data collected from internet pixels to build even more comprehensive profiles about the behavior and characteristics of millions of people.

55. Microsoft has several methods to collect data on users. For instance, Microsoft applications use additional identifiers, such as the Advertising ID in Windows.[39] "Windows generates a unique advertising ID for each person using a device, which app developers and advertising networks can then use for their own purposes, including providing relevant advertising in apps."[40] According to Microsoft, when the advertising ID is enabled, both Microsoft apps and third-party apps can access and use the advertising ID in much the same way that websites can access

[35] *Microsoft Privacy Statement*, Microsoft, https://www.microsoft.com/en-us/privacy/privacystatement#mainpersonaldatawecollectmodule (last updated Jan. 2025).

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

and use a unique identifier stored in a cookie.[41] Thus, a user's advertising ID can be used by app developers and advertising networks to provide "more relevant" advertising across their apps and on the Internet.[42]

B. The Bing Pixel

56. Microsoft owns and develops a second pixel, the Bing Pixel, which is similarly deployed on websites across the internet.

57. The Bing Pixel does not, itself facilitate real-time bidding. Instead, the Bing Pixel installs tracking cookies on the browsers of visitors to the websites where it is loaded and intercepts the content of user communications and other interactions with those websites.

58. The data collected by the Bing Pixel is similarly used by Defendants to add to its consumer data profiles and data advertising products described herein.

C. The Microsoft Surveillance Apparatus

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

1. Interception Of Communications

60. 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.

61. When the Adnxs Pixel or Bing 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.

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

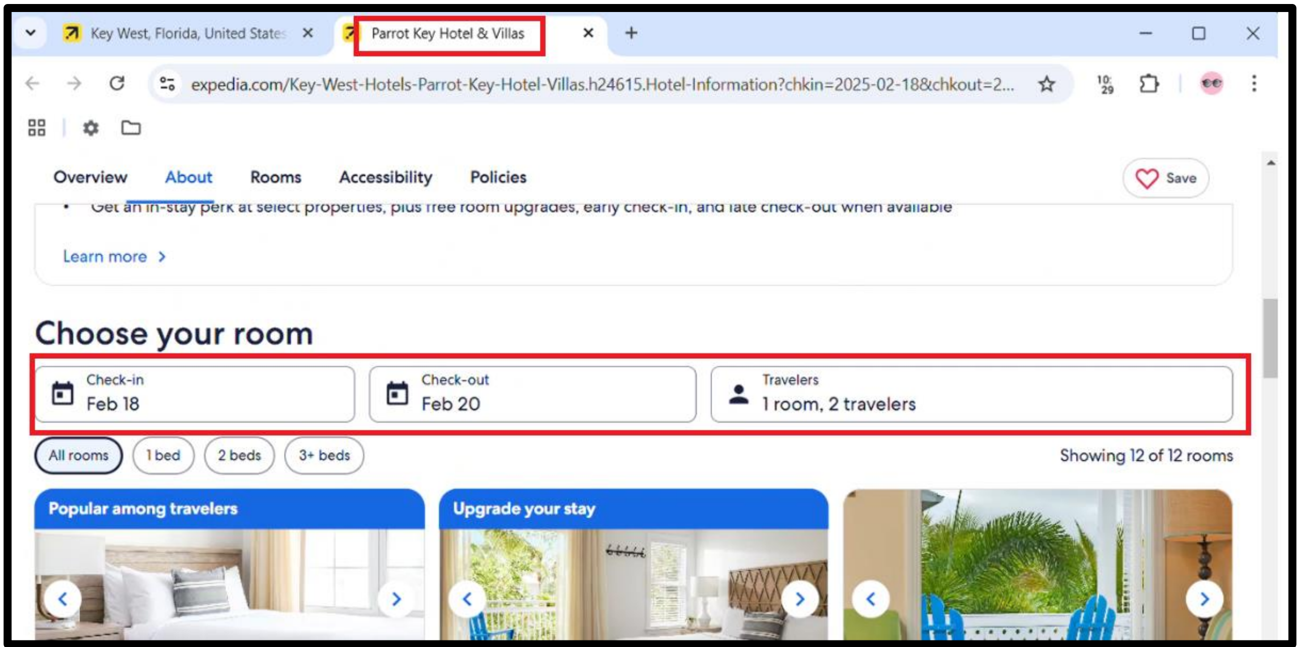
[41] *Id.*

[42] *Id.*

63. 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.

64. 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.

65. 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
Overview
About
Rooms
Accessibility
Policies
Save
Get an in-stay perk at select properties, plus free room upgrades, early check-in, and late check-out when available
Learn more
All rooms
1 bed
2 beds
3+ beds
Showing 12 of 12 rooms
Popular among travelers
Upgrade your stay

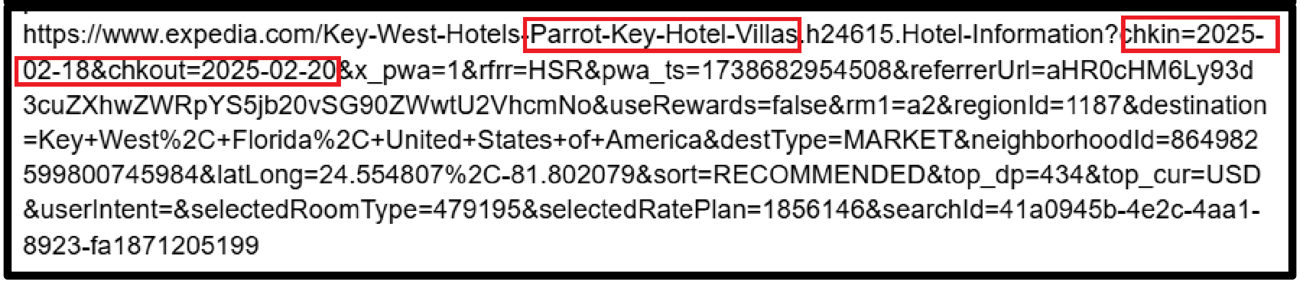
expedia.com/Key-West-Hotels-Parrot-Key-Hotel-Villas.h24615.Hotel-Information?chkin=2025-02-18&chkout=2...

Choose your room

Check-in Feb 18

Check-out Feb 20

Travelers 1 room, 2 travelers



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

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

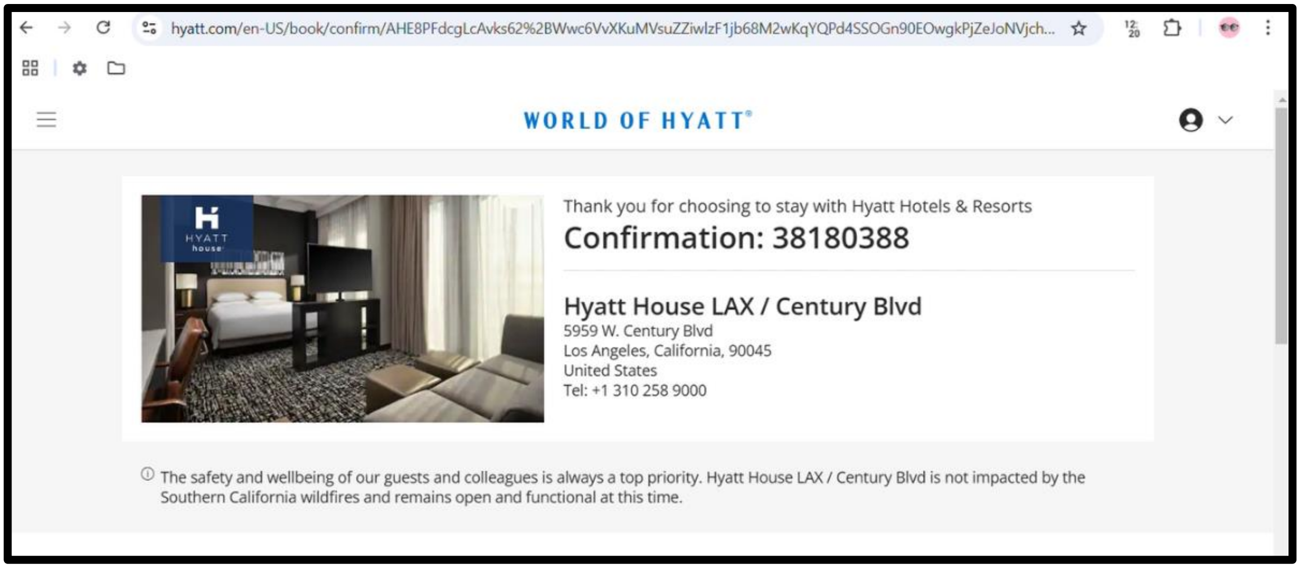
67. As such, any pixel that intercepts the URL on this page also intercepts the content of the users' communications with Expedia about their travel plans. This process works similarly on other websites.

68. The Microsoft pixels collect 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.

69. Further, with the Microsoft Pixels, Microsoft is able to keep track of users by tracking the referrer URL of the page the pixel was loaded from.[43] In even the most basic implementation of the pixels, Microsoft is able to track page views and identify the URLs driving them.[44] Because Microsoft tracks Internet users' URLs, it also tracks information from those URLs.

70. The Adnxs Pixel and Bing Pixel also intercept communications between individual internet users and websites that are not contained in the page URL.

71. 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

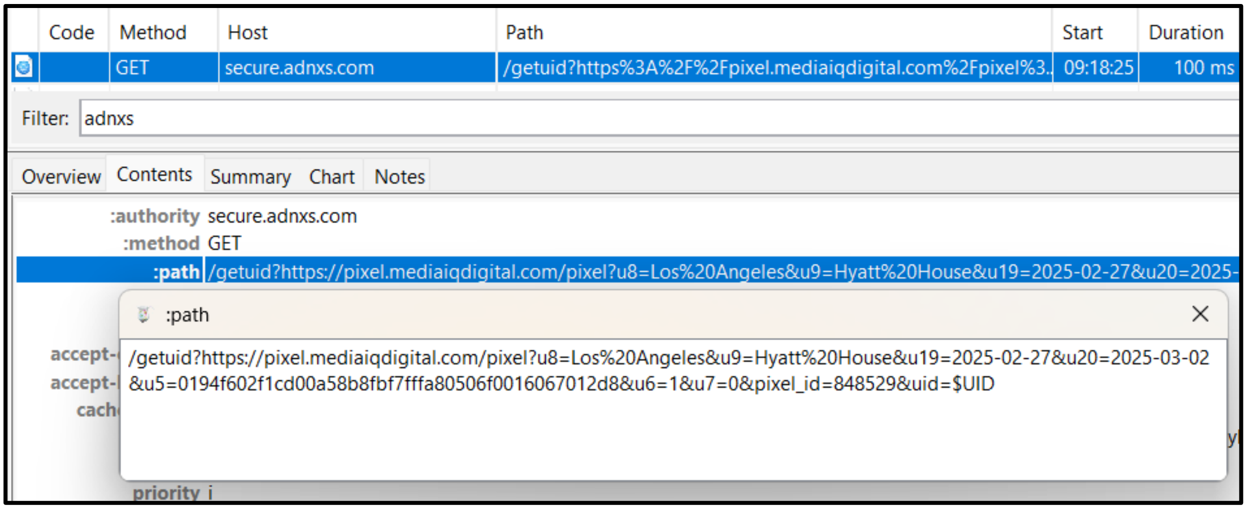
Confirmation: 38180388

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.

[43] *Microsoft Invest – Universal Pixel*, Microsoft (Oct. 14, 2024), https://learn.microsoft.com/en-us/xandr/invest/the-universal-pixel.

[44] *Microsoft Monetize – Universal Pixel Basic Implementation*, Microsoft (Feb. 7, 2024), https://learn.microsoft.com/en-us/xandr/monetize/universal-pixel-basic-implementation.



Code	Method	Host	Path	Start	Duration
	GET	secure.adnxs.com	/getuid?https%3A%2F%2Fpixel.mediaiqdigital.com%2Fpixel%3..	09:18:25	100 ms

Filter: adnxs

```
:authority secure.adnxs.com
   :method GET
     :path /getuid?https://pixel.mediaiqdigital.com/pixel?u8=Los%20Angeles&u9=Hyatt%20House&u19=2025-02-27&u20=2025-
```

:path

```
/getuid?https://pixel.mediaiqdigital.com/pixel?u8=Los%20Angeles&u9=Hyatt%20House&u19=2025-02-27&u20=2025-03-02
&u5=0194f602f1cd00a58b8fbf7fffa80506f0016067012d8&u6=1&u7=0&pixel_id=848529&uid=$UID
```

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

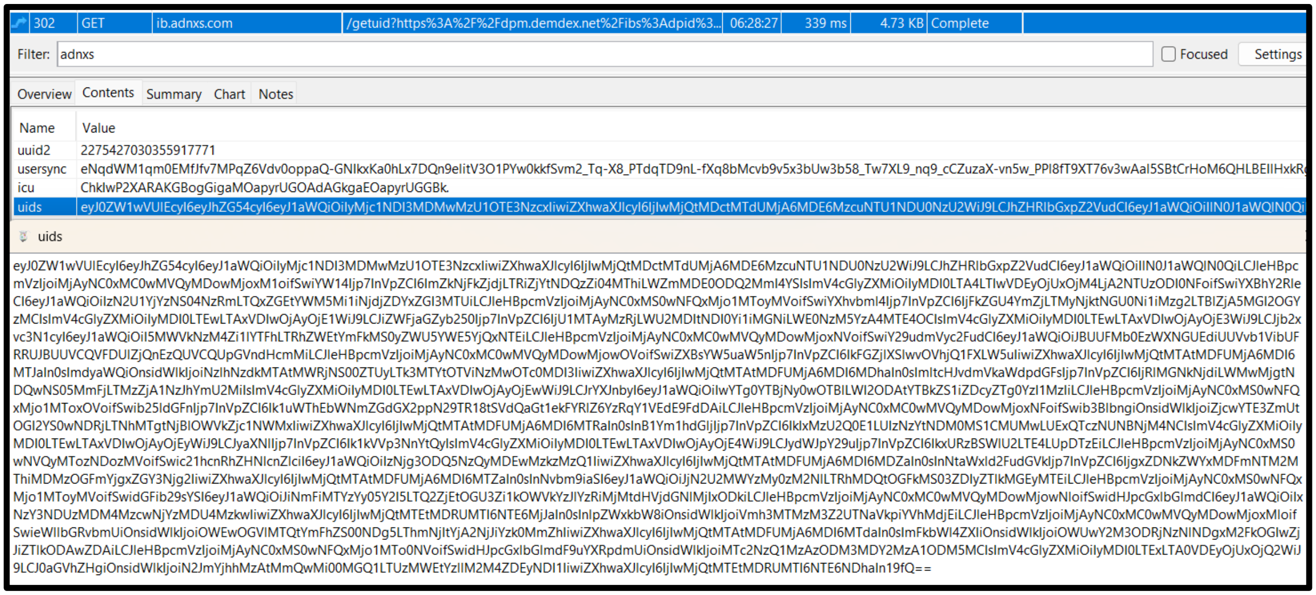
2. *Collection of Persistent Identifiers*

73. Another way Microsoft 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. Microsoft uses these identifiers to confirm that a person using a particular website is the same person identified by Microsoft on another website.

74. One form of persistent identifiers is a browser "cookie." "Cookies are bits of data that are sent to and from your browser to identify you. When you open a website, your browser sends a piece of data to the web server hosting that website."[45]

75. When the Adnxs Pixel or Bing Pixel is called onto a website, it automatically downloads a cookie onto the browser of the person visiting the website. Microsoft then links a proprietary ID number to the cookie and the individual with the cookie.

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



302 | GET | ib.adnxs.com | /getuid?https%3A%2F%2Fdpm.demdex.net%2Fibs%3Adpid%3... | 06:28:27 | 339 ms | 4.73 KB | Complete

Filter: adnxs □ Focused Settings

Overview Contents Summary Chart Notes

Name	Value
uuid2	2275427030355917771
usersync	eNqdWM1qm0EMfJfv7MPqZ6Vdv0oppaQ-GNIkxKa0hLx7DQn9eIitV3O1PYw0kkfSvm2_Tq-X8_PTdqTD9nL-fXq8bMcvb9v5x3bUw3b58_Tw7XL9_nq9_cCZuzaX-vn5w_PPI8fT9XT76v3wAaI5SBtCrHoM6QHLBEIIHxkR
icu	ChkIwP2XARAKGBogGigaMOapyrUGOAdAGkgaEOapyrUGGBk.
uids	eyJ0ZW1wVUlEcyI6eyJhZG54cyI6eyJ1aWQiOiIyMjc1NDI3MDMwMzU1OTE3NzcxIiwiZXhwaXJlcyI6IjIwMjQtMDctMTdUMjA6MDE6MzcuNTU1NDU0NzU2WiJ9LCJhZHRlbGxpZ2VudCI6eyJ1aWQiOiIlN0J1aWQlN0Qi

uids

```
eyJ0ZW1wVUlEcyI6eyJhZG54cyI6eyJ1aWQiOiIyMjc1NDI3MDMwMzU1OTE3NzcxIiwiZXhwaXJlcyI6IjIwMjQtMDctMTdUMjA6MDE6MzcuNTU1NDU0NzU2WiJ9LCJhZHRlbGxpZ2VudCI6eyJ1aWQiOiIlN0J1aWQlN0QiLCJleHBpc
mVzIjoiMjAyNC0xMC0wMVQyMDowMjoxM1oifSwiYW14Ijp7InVpZCI6ImZkNjFkZjdjLTRiZjYtNDQzZi04MThiLWZmMDE0ODQ2MmI4YSIsImV4cGlyZXMiOiIyMDI0LTA4LTIwVDEyOjUxOjM4LjA2NTUzODI0NFoifSwiYXBhY2Rle
CI6eyJ1aWQiOiIzN2U1YjYzNS04NzRmLTQxZGEtYWM5Mi1iNjdjZDYxZGI3MTUiLCJleHBpcmVzIjoiMjAyNC0xMS0wNFQxMjo1MToyMVoifSwiYXhvbmI4Ijp7InVpZCI6IjFkZGU4YmZjLTMyNjktNGU0Ni1iMzg2LTBlZjA5MGI2OGY
zMCIsImV4cGlyZXMiOiIyMDI0LTEwLTAxVDIwOjAyOjE1WiJ9LCJiZWFjaGZyb250Ijp7InVpZCI6IjU1MTAyMzRjLWU2MDItNDI0Yi1iMGNiLWE0NzM5YzA4MTE4OCIsImV4cGlyZXMiOiIyMDI0LTEwLTAxVDIwOjAyOjE3WiJ9LCJjb2x
vc3N1cyI6eyJ1aWQiOiI5MWVkNzM4Zi1lYTFhLTRhZWEtYmFkMS0yZWU5YWE5YjQxNTEiLCJleHBpcmVzIjoiMjAyNC0xMC0wMVQyMDowMjoxNVoifSwiY29udmVyc2FudCI6eyJ1aWQiOiJBUUFMb0EzWXNGUEdiUUVvb1VibUF
RRUJBUUVCQVFDUlZjQnEzQUVCQUpGVndHcmMiLCJleHBpcmVzIjoiMjAyNC0xMC0wMVQyMDowMjowOVoifSwiZXBsYW5uaW5nIjp7InVpZCI6IkFGZjlXSlwvOVhjQ1FXLW5uIiwiZXhwaXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6
MTJaIn0sImdyaWQiOnsidWlkIjoiNzlhNzdkMTAtMWRjNS00ZTUyLTk3MTYtOTViNzMwOTc0MDI3IiwiZXhwaXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6MDhaIn0sImltcHJvdmVkaWdpdGFsIjp7InVpZCI6IjRlMGNkNjdiLWMwMjgtN
DQwNS05MmFjLTMzZjA1NzJhYmU2MiIsImV4cGlyZXMiOiIyMDI0LTEwLTAxVDIwOjAyOjEwWiJ9LCJrYXJnbyI6eyJ1aWQiOiIwYTg0YTBjNy0wOTBlLWI2ODAtYTBkZS1iZDcyZTg0YzI1MzliLCJleHBpcmVzIjoiMjAyNC0xMS0wNFQ
xMjo1MToxOVoifSwib25ldGFnIjp7InVpZCI6Ik1uWThEbWNmZGdGX2ppN29TR18tSVdQaGt1ekFYRlZ6YzRqY1VEdE9FdDAiLCJleHBpcmVzIjoiMjAyNC0xMC0wMVQyMDowMjoxNFoifSwib3BlbngiOnsidWlkIjoiZjcwYTE3ZmUt
OGI2YS0wNDRjLTNhMTgtNjBlOWVkZjc1NWMxIiwiZXhwaXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6MTRaIn0sInB1Ym1hdGljIjp7InVpZCI6IkIxMzU2Q0E1LUIzNzYtNDM0MS1CMUMwLUExQTczNUNBNjM4NCIsImV4cGlyZXMiOiIy
MDI0LTEwLTAxVDIwOjAyOjEyWiJ9LCJyaXNlIjp7InVpZCI6Ik1kVVp3NnYtQyIsImV4cGlyZXMiOiIyMDI0LTEwLTAxVDIwOjAyOjE4WiJ9LCJydWJpY29uIjp7InVpZCI6IkxURzBSWlU2LTE4LUpDTzEiLCJleHBpcmVzIjoiMjAyNC0xMS0
wNVQyMTozNDozMVoifSwic21hcnRhZHNlcnZlciI6eyJ1aWQiOiIzNjg3ODQ5NzQyMDEwMzkzMzQ1IiwiZXhwaXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6MDZaIn0sInNtaWxld2FudGVkIjp7InVpZCI6IjgxZDNkZWYxMDFmNTM2M
ThiMDMzOGFmYjgxZGY3Njg2IiwiZXhwaXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6MTZaIn0sInNvbm9iaSI6eyJ1aWQiOiJjN2U2MWYzMy0zM2NlLTRhMDQtOGFkMS03ZDIyZTlkMGEyMTEiLCJleHBpcmVzIjoiMjAyNC0xMS0wNFQx
Mjo1MToyMVoifSwidGFib29sYSI6eyJ1aWQiOiJiNmFiMTYzYy05Y2I5LTQ2ZjEtOGU3Zi1kOWVkYzJlYzRiMjMtdHVjdGNlMjIxODkiLCJleHBpcmVzIjoiMjAyNC0xMC0wMVQyMDowMjowNloifSwidHJpcGxlbGlmdCI6eyJ1aWQiOiIx
NzY3NDUzMDM4MzcwNjYzMDU4MzkwIiwiZXhwaXJlcyI6IjIwMjQtMTEtMDRUMTI6NTE6MjJaIn0sInlpZWxkbW8iOnsidWlkIjoiVmh3MTMzM3Z2UTNaVkpiYVhMdjEiLCJleHBpcmVzIjoiMjAyNC0xMC0wMVQyMDowMjoxMloif
SwieWllbGRvbmUiOnsidWlkIjoiOWEwOGVlMTQtYmFhZS00NDg5LThmNjItYjA2NjJiYzk0MmZhIiwiZXhwaXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6MTdaIn0sImFkbWl4ZXIiOnsidWlkIjoiOWUwY2M3ODRjNzNlNDgxM2FkOGIwZj
JiZTlkODAwZDAiLCJleHBpcmVzIjoiMjAyNC0xMS0wNFQxMjo1MTo0NVoifSwidHJpcGxlbGlmdF9uYXRpdmUiOnsidWlkIjoiMTc2NzQ1MzAzODM3MDY2MzA1ODM5MCIsImV4cGlyZXMiOiIyMDI0LTExLTA0VDEyOjUxOjQ2WiJ
9LCJ0aGVhZHgiOnsidWlkIjoiN2JmYjhhMzAtMmQwMi00MGQ1LTUzMWEtYzllM2M4ZDEyNDI1IiwiZXhwaXJlcyI6IjIwMjQtMTEtMDRUMTI6NTE6NDhaIn19fQ==
```

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

77. After the cookie is loaded onto a person's browser, each time that person visits a website where a Microsoft pixel is called, Microsoft 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, Microsoft 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.

78. This information is cross-referenced with other information collected by Microsoft 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.

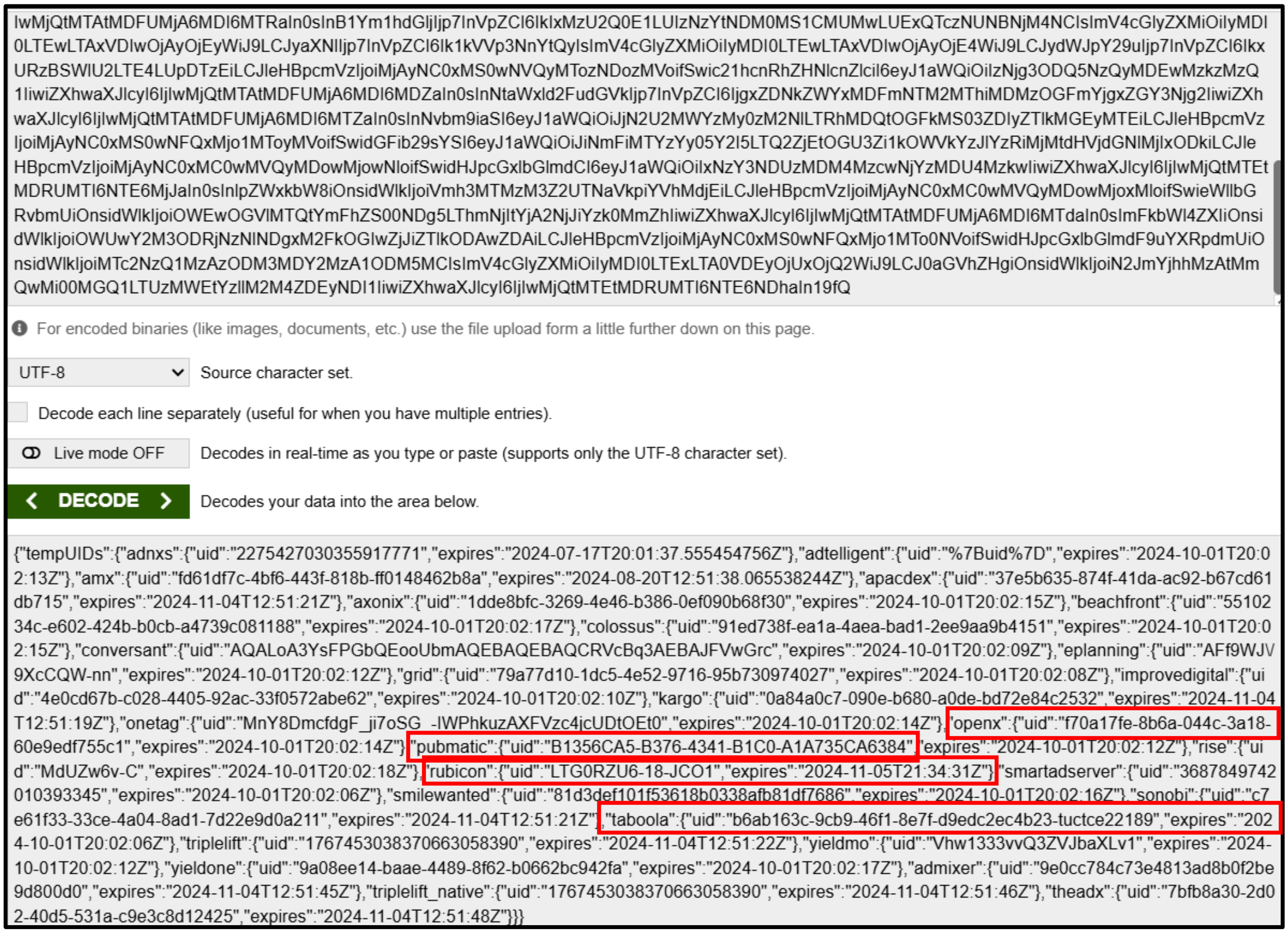
79. Microsoft associates users with several types of unique identifiers. The first is the "uuid2," which "identifiers a returning user's device" and is "used for targeted ads."[46]

80. The second is the "XANDR_PANID," which "registers data on the visitor" and "is used to optimize advertisement relevance."[47]

[46] TYSABRL, COOKIES, https://www.tysabri.com/en_us/cookies.html.

[47] *Id.*

81. The third is the "UIDS" parameter. The "UIDS" value is encoded in Base64, which can be easily decoded on publicly available websites.[48] Decoding the UIDS values above yields the user IDs for Partner Pixels that Microsoft's pixels are syncing with, which are then permanently stored with the cookie on the users' browsers. This allows Microsoft to identify the user based on other third party identifiers, and this value is constantly updated as Microsoft syncs with further third parties. For instance, the below screenshot shows the "UIDS" cookie includes identifiers for registered data brokers like PubMatic,[49] Magnite (Rubicon),[50] OpenX,[51] and Taboola[52]:



IwMjQtMTAtMDFUMjA6MDI6MTRaIn0sInB1Ym1hdGljIjp7InVpZCI6IkIxMzU2Q0E1LUIzNzYtNDM0MS1CMUMwLUExQTczNUNBNjM4NCIsImV4cGlyZXMiOiIyMDI
0LTEwLTAxVDIwOjAyOjEyWiJ9LCJyaXNlIjp7InVpZCI6Ik1kVVp3NnYtQyIsImV4cGlyZXMiOiIyMDI0LTEwLTAxVDIwOjAyOjE4WiJ9LCJydWJpY29uIjp7InVpZCI6Ikx
URzBSWlU2LTE4LUpDTzEiLCJleHBpcmVzIjoiMjAyNC0xMS0wNVQyMTozNDozMVoifSwic21hcnRhZHNlcnZlciI6eyJ1aWQiOiIzNjg3ODQ5NzQyMDEwMzkzMzQ
1IiwiZXhwaXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6MDZaIn0sInNtaWxld2FudGVkIjp7InVpZCI6IjgxZDNkZWYxMDFmNTM2MThiMDMzOGFmYjgxZGY3Njg2IiwiZXh
waXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6MTZaIn0sInNvbm9iaSI6eyJ1aWQiOiJjN2U2MWYzMy0zM2NlLTRhMDQtOGFkMS03ZDIyZTlkMGEyMTEiLCJleHBpcmVz
IjoiMjAyNC0xMS0wNFQxMjo1MToyMVoifSwidGFib29sYSI6eyJ1aWQiOiJiNmFiMTYzYy05Y2I5LTQ2ZjEtOGU3Zi1kOWVkYzJlYzRiMjMtdHVjdGNlMjIxODkiLCJle
HBpcmVzIjoiMjAyNC0xMC0wMVQyMDowMjowNloifSwidHJpcGxlbGlmdCI6eyJ1aWQiOiIxNzY3NDUzMDM4MzcwNjYzMDU4MzkwIiwiZXhwaXJlcyI6IjIwMjQtMTEt
MDRUMTI6NTE6MjJaIn0sInlpZWxkbW8iOnsidWlkIjoiVmh3MTMzM3Z2UTNaVkpiYVhMdjEiLCJleHBpcmVzIjoiMjAyNC0xMC0wMVQyMDowMjoxMloifSwieWllbG
RvbmUiOnsidWlkIjoiOWEwOGVlMTQtYmFhZS00NDg5LThmNjItYjA2NjJiYzk0MmZhIiwiZXhwaXJlcyI6IjIwMjQtMTAtMDFUMjA6MDI6MTdaIn0sImFkbWl4ZXIiOnsi
dWlkIjoiOWUwY2M3ODRjNzNlNDgxM2FkOGIwZjJiZTlkODAwZDAiLCJleHBpcmVzIjoiMjAyNC0xMS0wNFQxMjo1MTo0NVoifSwidHJpcGxlbGlmdF9uYXRpdmUiO
nsidWlkIjoiMTc2NzQ1MzAzODM3MDY2MzA1ODM5MCIsImV4cGlyZXMiOiIyMDI0LTExLTA0VDEyOjUxOjQ2WiJ9LCJ0aGVhZHgiOnsidWlkIjoiN2JmYjhhMzAtMm
QwMi00MGQ1LTUzMWEtYzllM2M4ZDEyNDI1IiwiZXhwaXJlcyI6IjIwMjQtMTEtMDRUMTI6NTE6NDhaIn19fQ

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

{"tempUIDs":{"adnxs":{"uid":"2275427030355917771","expires":"2024-07-17T20:01:37.555454756Z"},"adtelligent":{"uid":"%7Buid%7D","expires":"2024-10-01T20:0
2:13Z"},"amx":{"uid":"fd61df7c-4bf6-443f-818b-ff0148462b8a","expires":"2024-08-20T12:51:38.065538244Z"},"apacdex":{"uid":"37e5b635-874f-41da-ac92-b67cd61
db715","expires":"2024-11-04T12:51:21Z"},"axonix":{"uid":"1dde8bfc-3269-4e46-b386-0ef090b68f30","expires":"2024-10-01T20:02:15Z"},"beachfront":{"uid":"55102
34c-e602-424b-b0cb-a4739c081188","expires":"2024-10-01T20:02:17Z"},"colossus":{"uid":"91ed738f-ea1a-4aea-bad1-2ee9aa9b4151","expires":"2024-10-01T20:0
2:15Z"},"conversant":{"uid":"AQALoA3YsFPGbQEooUbmAQEBAQEBAQCRVcBq3AEBAJFVwGrc","expires":"2024-10-01T20:02:09Z"},"eplanning":{"uid":"AFf9WJV
9XcCQW-nn","expires":"2024-10-01T20:02:12Z"},"grid":{"uid":"79a77d10-1dc5-4e52-9716-95b730974027","expires":"2024-10-01T20:02:08Z"},"improvedigital":{"ui
d":"4e0cd67b-c028-4405-92ac-33f0572abe62","expires":"2024-10-01T20:02:10Z"},"kargo":{"uid":"0a84a0c7-090e-b680-a0de-bd72e84c2532","expires":"2024-11-04
T12:51:19Z"},"onetag":{"uid":"MnY8DmcfdgF_ji7oSG_-IWPhkuzAXFVzc4jcUDtOEt0","expires":"2024-10-01T20:02:14Z"},"openx":{"uid":"f70a17fe-8b6a-044c-3a18-
60e9edf755c1","expires":"2024-10-01T20:02:14Z"},"pubmatic":{"uid":"B1356CA5-B376-4341-B1C0-A1A735CA6384","expires":"2024-10-01T20:02:12Z"},"rise":{"ui
d":"MdUZw6v-C","expires":"2024-10-01T20:02:18Z"},"rubicon":{"uid":"LTG0RZU6-18-JCO1","expires":"2024-11-05T21:34:31Z"},"smartadserver":{"uid":"3687849742
010393345","expires":"2024-10-01T20:02:06Z"},"smilewanted":{"uid":"81d3def101f53618b0338afb81df7686","expires":"2024-10-01T20:02:16Z"},"sonobi":{"uid":"c7
e61f33-33ce-4a04-8ad1-7d22e9d0a211","expires":"2024-11-04T12:51:21Z"},"taboola":{"uid":"b6ab163c-9cb9-46f1-8e7f-d9edc2ec4b23-tuctce22189","expires":"202
4-10-01T20:02:06Z"},"triplelift":{"uid":"1767453038370663058390","expires":"2024-11-04T12:51:22Z"},"yieldmo":{"uid":"Vhw1333vvQ3ZVJbaXLv1","expires":"2024-
10-01T20:02:12Z"},"yieldone":{"uid":"9a08ee14-baae-4489-8f62-b0662bc942fa","expires":"2024-10-01T20:02:17Z"},"admixer":{"uid":"9e0cc784c73e4813ad8b0f2be
9d800d0","expires":"2024-11-04T12:51:45Z"},"triplelift_native":{"uid":"1767453038370663058390","expires":"2024-11-04T12:51:46Z"},"theadx":{"uid":"7bfb8a30-2d0
2-40d5-531a-c9e3c8d12425","expires":"2024-11-04T12:51:48Z"}}}

[48] *See, e.g.*, https://www.base64decode.org/.

[49] Data Broker Registration for PubMatic, Inc., https://oag.ca.gov/data-broker/registration/186702.

[50] Data Broker Registration for Magnite Inc., https://oag.ca.gov/data-broker/registration/568127.

[51] Data Broker Registration for OpenX Technologies, Inc., https://oag.ca.gov/data-broker/registration/193614.

[52] Data Broker Registration for Taboola, Inc., https://oag.ca.gov/data-broker/registration/186589.

a. IP Addresses

82. IP addresses are another common persistent identifier.

83. 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.[53]

84. 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.

85. 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.

86. 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.[54] Thus, knowing a user's public IP address—and therefore geographical location—"provide[s] a level of specificity previously unfound in marketing."[55]

87. An IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[56] and (ii) "to target specific households, businesses[,] and even

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

[54] *IP Location Lookup*, iplocation.io, https://iplocation.io/ (last accessed Feb. 12, 2025).

[55] *IP Targeting: Understanding This Essential Marketing Tool*, AccuData (Nov. 20, 2023), https://web.archive.org/web/20231209011353/https://www.accudata.com/blog/ip-targeting/.

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

individuals with ads that are relevant to their interests."[57] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[58] because "[c]ompanies can use an IP address … to personally identify individuals."[59]

88. In fact, an IP address is a common identifier used for "geomarketing," which is "the practice of using location data to identify and server 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."[60] For example, for a job fair in a specific city, companies can send advertisements to only those in the general location of the upcoming event.[61]

89. "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."[62]

90. "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."[63]

91. 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

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

[58] *IP Targeting: Understanding This Essential Marketing Tool*, *supra*.

[59] 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/.

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

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

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

[63] *Id*.

of advertising."[64] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[65]

92. Further, "IP address targeting can help businesses to improve their overall marketing strategy."[66] "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."[67]

93. Putting IP addresses in the hands of the data brokers who sync with Microsoft 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.[68]

94. 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."[69]

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

95. Microsoft employs similar methods to track individuals using mobile apps on Android and iOS devices.

[64] Williams, *supra* note 39.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] Twetman & Bergmanis-Korats, *supra* note 4.

[69] *Is an IP Address Personal Data?* Convesio, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/ (last modified June 22, 2024); *see also Data Protection Explained*, European Commission, https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en (last accessed Feb. 12, 2025).

96. Microsoft 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.[70]

97. 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."[71]

98. An API "acts as an intermediary layer that processes data transfer between systems, letting companies open their application data and functionality to external third-party developers [and] business partners."[72] An API can "work[] as a standalone solution or included within an SDK … [A]n SDK often contains at least one API."[73] 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."[74]

99. Similar to the pixels on web browsers, the Microsoft SDKs are called by other SDKs when a user accesses a particular app.

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

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

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

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

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

[73] IBM, *supra* note 52.

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

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

102. An AAID is a unique string of numbers that attaches to a device. As the name implies, an AAID is sent to advertisers and other third parties so they can track user activity across multiple mobile applications.[75] 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.

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

104. Using publicly available resources, an AAID can track a user's movements, habits, and activity on mobile applications.[76] Put together, the AAID serves as "the passport for aggregating all of the data about a user in one place."[77]

105. 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

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

[76] 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.

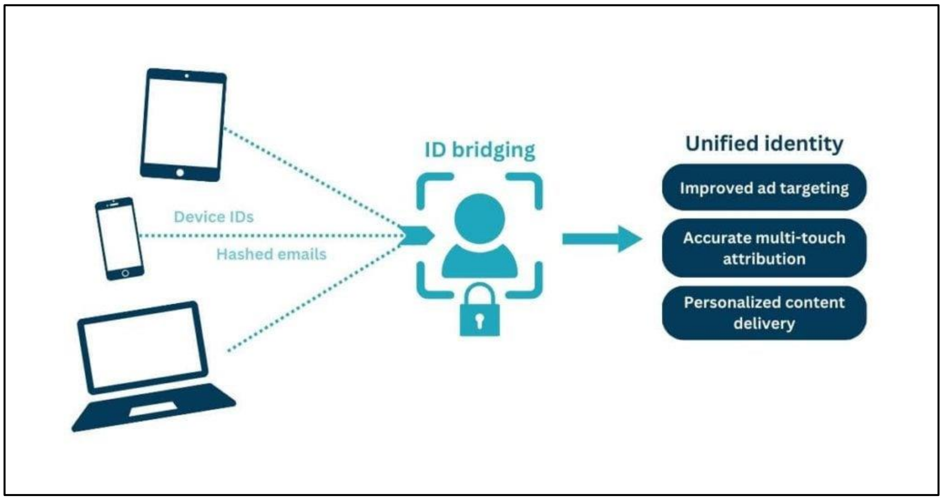
[77] *Trend Report: Apps Oversharing Your Advertising ID*, International Digital Accountability Council, https://digitalwatchdog.org/trend-report-apps-oversharing-your-advertising-id/ (last accessed Feb. 13, 2025).

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.

106. 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."[78]

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

108. 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."[79] 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.



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

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

109. ID Bridging "has long been the foundation of the programmatic advertising,"[80] 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."[81] It entails a "unique identifier [] assigned to individual devices," including Google's Advertising ID," personal information like geolocation and e-mail address, and "cross-platform linkage."[82]

110. 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."[83]

111. 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.

112. Many companies (*e.g.*, data brokers, identity graph providers), publicly advertise their ability to conduct such bridging. Yet, while those within the ID Bridging industry describe it as privacy-protective, it is anything but. As courts have noted, the "ability to amass vast amounts of personal data for the purpose of identifying individuals and aggregating their many identifiers" creates "dossiers which can be used to further invade [users] privacy by allowing third parties to learn intimate details of [users'] lives, and target them for advertising, political, and other purposes, ultimately harming them through the abrogation of their autonomy and their ability to control

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

[81] *Programmatic Advertising*, Amazon, https://advertising.amazon.com/blog/programmatic-advertising# (last accessed Feb. 13, 2025).

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

[83] 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.

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).

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

> a consumer's "shadow profile" [is a] massive, largely hidden dataset[] of online and offline activities. This information is collected through an extensive web of … services, which is difficult, if not impossible to avoid. It is largely collected invisibly and without consumer consent. Processed by algorithms and artificial intelligence, this data reveals an intimate picture of a specific consumer's movements, socio-economics, demographics, "likes", activities and more. It may or may not be associated with a specific users' name, but the specificity of this information defines the individual in such detail that a name is unnecessary.[84]

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

c. <u>Other Identifiers</u>

115. In addition to the methods described above, which are explicitly designed to track individuals across different devices and apps, Microsoft collects other identifying information that allows it to determine whether the same individual is visiting multiple websites or using multiple apps where Microsoft technology is called to or installed directly.

116. One method is through collecting e-mail addresses. The logic of this is straightforward. If Microsoft 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.

117. 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.

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

118. HTTP requests, when intercepted by Microsoft, 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.

3. User ID Mapping with getUID and mapUID

119. Microsoft offers tools so that its clients can identify the users they track. Microsoft provides its clients with technology that allows them to sync user ID information to have a user ID associated with all users in all ad calls.[85] Microsoft used the Adnxs Pixel to sync user IDs with supply partners, demand partners, and data providers.[86]

120. According to Microsoft, when it gets an ad call, it has "to know the user's Microsoft Advertising user ID so that [it] can apply frequency and regency, segment, and other data.[87] [Microsoft] can easily do this when [Microsoft's] tag is on the page (*i.e.*, the tag domain is ib.adnxs.com or has been CNAMEd to ib.adnsx.com) because [Microsoft] can access the user's ib.adnxs.com browser cookie where [Microsoft] store[s] an Microsoft Advertising ID."[88]

121. For bidders, Microsoft states it "initiates the usersyncing process with external bidders because these bidders need to be able to make purchasing decisions based on their own user data."[89] As for data providers, Microsoft syncs "with data providers because they send [Microsoft] more data to bid on. This leads to making better bidding decisions based on having better information available."[90]

[85] *User ID Synching with External Partners*, Microsoft (Feb. 2, 2024), https://learn.microsoft.com/en-us/xandr/monetize/user-id-syncing-with-external-partners,

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *Id.*

122. Microsoft is able to sync user IDs through two pixels: mapUID and getUID.[91] The mapUID services passes Microsoft's clients' internal ID to Microsoft for mapping to the Microsoft Advertising ID within the Microsoft Advertising cookie store.[92]

123. The average time to live for mapUID mappings is around 2.5 weeks. Thus, Microsoft stresses the importance of its clients firing the mapUID pixel "as frequently as possible and on as many pages as possible to keep [the] mappings live."[93]

124. The getUID service, initiated on websites by the Adnxs Pixel retrieves the Microsoft Advertising ID so Microsoft's clients can coordinate it with their own in-house ID server side or their own cookie space.[94] Then Microsoft clients can pass in an offline data feed that says, "update Microsoft Advertising user ABC with the following segment data."[95]

125. The getUID service is Microsoft's version of a data sharing practice known as "identity resolution"

126. In plain language, identity resolution is another way to monetize Microsoft's tracking, where it assigns am 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.

127. 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.

128. This process happens when both the Adnxs Pixel and a Partner Pixel are loaded onto a website. The Partner Pixel "calls" the Adnxs Pixel and the Adnxs Pixel responds with a getUID

[91] *Microsoft Invest – User ID Mapping with getUID and mapUID*, Microsoft (Feb. 23, 2024), https://learn.microsoft.com/en-us/xandr/invest/user-id-mapping-with-getuid-and-mapuid#getuid-service.

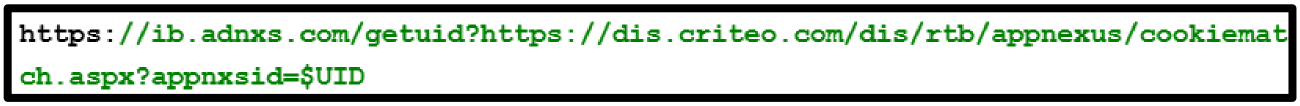
[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

request that shares the individual's Microsoft ID and associated information, including the identifiers described above, with that Partner Pixel.



```
https://ib.adnxs.com/getuid?https://dis.criteo.com/dis/rtb/appnexus/cookiematch.aspx?appnxsid=$UID
```

129. This process happens multiple times on each website, with many tracking pixels and potential advertisers gaining access to an individual's information for bidding and targeted advertising, enriching Defendant, the other technology companies involved, and the host websites alike while trampling consumer privacy in the process. Transmissions of this type are happening across all of the websites and apps where the Adnxs pixel is loaded.

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

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

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

133. 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 Microsoft. 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*.

134. Specifically, Plaintiffs' counsel found that each website and/or app had Partner Pixels loaded onto it, which in turn communicated with the Adnxs pixel to better enable their advertising. Each Partner Pixel would itself intercept users' communications with the website or app. The Adnxs pixel would then assign a Microsoft ID to the user's activity on the website or app, which, among

other things, (i) allowed for the user to be identified; (ii) link the user to information from across other websites and apps; and (iii) benefit the websites, apps, and Partner Pixels by making that user more valuable to advertisers because the user could be better targeted with relevant ads due to the extensive information Defendant collected and provided to the Partner Pixels.

B. Xandr

135. Xandr, formerly known as AppNexus, is a real-time bidding advertising platform powered by Microsoft. Xandr offers products and services for "executing programmatic advertising campaigns across screens and tapping into engaged audiences."[96] In other words, Xandr offers a portfolio of advertising and analytics products and services that provide Microsoft's clients the technology to buy and sell digital advertising space, data management, and analytics tools.[97] Xandr's features include real-time bidding, programmatic buying … as well as tools for creative optimization and audience targeting … and solutions for video and mobile advertising."[98] Xandr achieves this through three products: Microsoft Invest, Microsoft Monetize, and Microsoft Curate. Xandr is both a demand-side platform and a supply-side platform.[99]

136. Xandr partners with third-party providers who receive platform data and other consumer information (however, the extent of this data is unknown as it is confidential and tied to specific contracts between Xandr and its customers[100]).[101]

137. As a result, Xandr shares information about consumers with over a thousand ad-server partners, hundreds of bidder partners, and 115 user sync providers. [102] Xandr's bidders receive full

[96] *Xandr Platform Documentation*, Microsoft, https://learn.microsoft.com/en-us/xandr/ (last accessed Feb. 10, 2025).

[97] *What is Xandr?* Zuuvi, https://www.zuuvi.com/display-advertising-platforms/xandr (last accessed Feb. 10, 2025).

[98] *Id*.

[99] *Differences Between DSPs, SSPs, and DMPs in Advertising*, SetupAd (Sept. 25, 2024), https://setupad.com/blog/dsp-vs-ssp (last accessed Feb. 10, 2025).

[100] *Policies and Regulations*, Microsoft, https://learn.microsoft.com/en-us/xandr/policies-regulations/ (last accessed Feb. 10, 2025).

[101] *Third Party Providers*, Microsoft (Feb. 7, 2024), https://learn.microsoft.com/en-us/xandr/policies-regulations/third-party-providers.

[102] *Id*.

details of every auction the bid request.[103] These details include: auction ID, Xandr user ID, referrer URL (usually the URL of a webpage visited by the individual), IP address, data about a user collected by Microsoft (known as "segment information"), data about a user that has been shared by another data provider.[104]

1. Microsoft Invest

138. Microsoft Invest is a "strategic buying platform built for the needs of today's advertisers looking to invest in upper-funnel buying and drive business results."[105] This means that Microsoft Invest is a tool aimed at the beginning of a consumer's journey, where a consumer begins to find information on products or services needed or desired.[106] "This is possibly the most critical step in the funnel because potential consumers have the tendency to turn toward the business most effective at capturing their attention."[107]

139. Microsoft Invest "is an end-to-end, integrated platform across the buy and sell side, which provides a number of benefits to users, including: seamless integration with major ad networks, exchanges, and aggregators[;] [s]treamlined, direct access to premium omnichannel supply[; and r]educed discrepancies and optimal match rates on [their] platform supply."[108]

140. Microsoft Invest features the Microsoft Advertising platform, which is a real-time bidding system and ad server.[109] The main processing system of the platform receives ad requests, applies data to the request, receives bids, makes decisions, serves creatives, and logs auctions, among other functions.[110]

[103] *Xandr's Bidders*, Microsoft (Feb. 27, 2024), https://learn.microsoft.com/en-us/xandr/data-providers/segment-usage-by-buyers#xandrs-bidders.

[104] *Id.*

[105] *About Microsoft Invest*, Microsoft, https://learn.microsoft.com/en-us/xandr/invest/about-invest (last accessed Feb. 10, 2025).

[106] Matt Colborn, *Upper Funnel vs. Lower Funnel*, Matrix Point, https://www.thematrixpoint.com/resources/articles/upper-funnel-vs-lower-funnel (last accessed Feb. 10, 2025).

[107] *Id.*

[108] *About Microsoft Invest*, Microsoft, https://learn.microsoft.com/en-us/xandr/invest/about-invest (last accessed Feb. 10, 2025).

[109] *Id.*

[110] *Id.*

141. Microsoft Invest offers the "universal pixel"—a pixel that provides insights into the interaction that users have with a website, so that Microsoft clients can easily segment, *i.e.*, identify the users and measure the value of the actions they take.[111] According to Microsoft, the universal pixel removes the need to separately define conversion pixels and segment pixels.[112] Defendant's clients implement the pixel by placing the code on their website.[113] With the universal pixel, Defendant's clients are able to keep track of users by tracking the referrer URL of the page the pixel was loaded from, track standard events based on user actions on a page, and track additional metadata that is passed using a parameter along with a standard event.[114] The universal pixel enables Defendant and Defendant's clients who use the pixel to track and target consumers on the Internet.

2. Microsoft Monetize

142. Another product that Microsoft offers to track individuals on the Internet, is Microsoft Monetize. Microsoft Monetize is "a sophisticated ad management technology platform with both buy- and sell-side capabilities.[115] Microsoft Monetize is built on an API, the Digital Platform API, which allows Microsoft's clients to buy and sell ad space on a single, unified interface.[116][117]

143. Through Microsoft Monetize, Defendant offers a "segment pixel," which is "placed on web pages to collect data about users, such as pages they visit, actions they take, or qualities such as gender, location, and wealth."[118] Further, "when a segment pixel fires, the user is added to a

[111] *Microsoft Invest – Universal Pixel*, Microsoft (Oct. 14, 2024), https://learn.microsoft.com/en-us/xandr/invest/the-universal-pixel.

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Network Guide*, Microsoft (Mar. 2, 2024), https://learn.microsoft.com/en-us/xandr/monetize/network-guide.

[116] *Monetize API*, Microsoft (Mar. 4, 2024), https://learn.microsoft.com/en-us/xandr/monetize/digital-platform-ui-api-info.

[117] *About Microsoft Monetize*, Microsoft (May 10, 2024), https://learn.microsoft.com/en-us/xandr/monetize/about-monetize.

[118] *Microsoft Monetize – Object Hierarchy*, Microsoft (Nov. 3, 2024), https://learn.microsoft.com/en-us/xandr/monetize/object-hierarchy.

segment, which can later be targeted in line items to attempt to reach the user again (retargeting)."[119] In this way**, users are perpetually tracked, identified and targeted or "retargeted"** over and over.

144. Defendant's clients have "many different options for targeting users in [their] line items and campaigns."[120] Some options Defendant offers include "targeting based on geography, domain, and inventory type" and through defining custom keys and values.[121] "Key/value targeting allows [clients] to take information [they have] collected and target [their] line items or campaigns to specific sets of users based on that information."[122]

145. As Defendant explains, a key is a category, such as the information a client has on the types of music users listen to or the types of cars they drive.[123] As such, "music_genre" and "car_type" could be custom keys.[124] A value is a specific instance of the key. For instance, the music_genre key could have values such as rock, jazz, and classical and the car_type key could include sedan, coupe, and SUV.[125]

146. This demonstrates not only that Defendant enables its clients to access vast amounts of detailed information Defendant collects on users, but also that Defendant's clients are able to quickly and easily customize and sift through that data.

147. But the ways that Microsoft Monetize offers to track users do not stop there. Microsoft Monetize offers Defendant's clients the "conversion pixel" to track user actions on a webpage such as registering at a site or making a purchase; "the third-party creative pixel" to trigger a third-party action like performing ad verification or collecting data about the creative (which is an advertising unit created by a client for the purpose of communicating a marketing message to that client's audience and can include images, animation, video, interactive experiences or more) when a

[119] *Id.*

[120] *Getting Started with Key/Value Targeting*, Microsoft (Mar. 2, 2024), https://learn.microsoft.com/en-us/xandr/monetize/getting-started-with-key-value-targeting.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Id.*

creative is served; an "impression tracker" to track impressions associated with creatives that are hosted by non-Microsoft Advertising ad servers by attaching the tracker as a "piggyback pixel" on the externally hosted creative; and a "click tracker" to track clicks associated with creatives that are hosted by non-Microsoft Advertising ad servers by also attaching the tracker as a "piggyback pixel" on the externally hosted creative;[126] and the "universal pixel" as discussed above,[127] where even the most basic implementation of the universal pixel allows Microsoft's client to track page views and identify the URLs driving them.[128]

148. The pixel can be configured to identify events the client wants captured, such as adding an item to a shopping cart[129] or tracking when a user enters payment information at checkout.[130]

149. After Microsoft's clients have set up a standard or custom event, they can use the data collected to identify audiences and conversions.[131] An audience, or audience segment, consists of a collection of users who have interacted on a website in a similar way.[132] After one or more audiences are configured, Microsoft's clients can target the audience from a line item.[133] A conversion, however, is a "specific type of interaction that indicates the successful downstream effects of an ad campaign"[134] or in other words, the website user's behavior on the website conformed with what the website owner wanted the user to do.

[126] *Microsoft Monetize – Object Hierarchy*, *supra* note 46.

[127] *Microsoft Invest – Universal Pixel*, Microsoft (Oct. 14, 2024), https://learn.microsoft.com/en-us/xandr/invest/the-universal-pixel.

[128] *Microsoft Monetize – Universal Pixel Basic Implementation*, Microsoft (Feb. 7, 2024), https://learn.microsoft.com/en-us/xandr/monetize/universal-pixel-basic-implementation.

[129] *Microsoft Monetize – Using Events and Parameters*, Microsoft (Mar. 7, 2024), https://learn.microsoft.com/en-us/xandr/monetize/using-events-and-parameters.

[130] *Microsoft Monetize – Standard Events and Parameters*, Microsoft (Mar. 6, 2024), https://learn.microsoft.com/en-us/xandr/monetize/standard-events-and-parameters.

[131] *Microsoft Monetize – Universal Pixel Audiences and Conversions*, Microsoft (Feb. 7, 2024), https://learn.microsoft.com/en-us/xandr/monetize/universal-pixel-audiences-and-conversions.

[132] *Id.*

[133] *Id.*

[134] *Id.*

150. Microsoft Monetize, through Microsoft Advertising, attributes conversion to a specific user and is able to tell Microsoft's clients whether the user has converted in response to having previously viewed or clicked one of the advertiser's creatives.[135] The universal pixel lets Microsoft's clients set up highly specific audiences and conversions based on complex rules.[136] For instance, Microsoft's client "might determine that a user who has clicked through to an offer, viewed three or more TVs, and accessed product details for a TV that cost over $1000 should be added to an audience segment called High-End TV Buyers."[137]

151. Defendant's targeting tools can be so precise that it allows its clients to add or remove a user from one or more segments at the same time a conversion pixel is fired.[138] Segmenting users after conversion is done, for example, when Microsoft's clients do not want to advertise to users who have already purchased a product.[139] In this way, users across the Internet are tracked and identified by some means.

152. Microsoft Monetize also offers what it calls "birthday cookies."[140] This is the codename for the "stamping" and ID syncing process described above. The first time a user without one of Microsoft's cookie visits a website where a Microsoft pixel is loaded, Microsoft sets a cookie.[141] Defendant also adds that user to the "Microsoft Advertising Birthday Cookie" segment, where the segment is exposed to all members of the platform and any member of the platform can use the segment.[142]

[135] *Microsoft Monetize – Conversion Attribution*, Microsoft (Feb. 26, 2024), https://learn.microsoft.com/en-us/xandr/monetize/conversion-attribution.

[136] *Microsoft Monetize – Universal Pixel Audiences and Conversions*, Microsoft (Feb. 7, 2024), https://learn.microsoft.com/en-us/xandr/monetize/universal-pixel-audiences-and-conversions.

[137] *Id.*

[138] https://learn.microsoft.com/en-us/xandr/monetize/conversion-pixels-advanced (last accessed Feb. 10, 2025).

[139] *Id.*

[140] *Microsoft Monetize – Birthday Cookies*, Microsoft (Mar. 1, 2024), https://learn.microsoft.com/en-us/xandr/monetize/birthday-cookies.

[141] *Id.*

[142] *Id.*

153. Through its Microsoft Advertising cookie store, **Defendant is able to both recognize any given user and access their relevant user data across multiple sites and platforms**.[143] The Microsoft Advertising cookie store is a server-side user data storage system that allows Defendant to sync user ID and frequency data across all Microsoft Advertising supply partners and store cookie data, both from Microsoft and Microsoft's clients, server side, so that it is accessible on every ad call.[144] This allows Microsoft to "maintain consistent and comprehensive data about a user no matter where, when, or how [Microsoft is] 'seeing' them across the Internet landscape."[145]

154. Further yet, Microsoft Monetize enables its clients to target based on location.[146] "A geo radius segment is a list of latitude, longitude, and radius data"[147] and this data provides enough information to locate and individual user. Microsoft Monetize allows its clients to use geo radius segments for "geographical targeting of multiple user locations."[148]

3. Microsoft Curate

155. Microsoft Curate is another program offered by Microsoft. Microsoft Curate allows curators to use their proprietary assets to enhance the value of a seller's inventory and create unique offerings for buyers.[149] Curators such as retailers, data companies, independent trading desks, and other media companies can use Microsoft Curate's features to centralize their business rules and targeting configurations across DSPs to simplify their campaign execution.[150]

[143] *Microsoft Monetize – Server Side Cookie Store*, Microsoft (Mar. 6, 2024), https://learn.microsoft.com/en-us/xandr/monetize/server-side-cookie-store.

[144] *Id.*

[145] *Id.*

[146] *Microsoft Monetize – Geo Radius Segments*, Microsoft (Mar. 2, 2024), https://learn.microsoft.com/en-us/xandr/monetize/geo-radius-segments.

[147] *Id.*

[148] *Id.*

[149] *About Microsoft Curate*, Microsoft (Feb. 12, 2024), https://learn.microsoft.com/en-us/xandr/curate/about-curate.

[150] *Id.*

156. Another feature of Microsoft Curate is that it allows Microsoft's clients, whether buyers or sellers, to interact with each other.[151] Microsoft Curate offers a platform where Microsoft's clients can discover new partners, cultivate relationships by communicating directly in Curate, motivate partners to do business with a client, and track success of partnerships with metrics.[152] Microsoft Curate also offers a feature where Microsoft's clients can "target users based on the day and time when they see impressions."[153]

157. Like Microsoft Invest and Microsoft Monetize, Microsoft Curate offers tools to target users on the Internet. With system targeting on Microsoft Curate, Defendant's clients can "target users based on [that user's] operating systems, browsers, language, device model, or carrier."[154] Moreover, Microsoft Curate clients can target mobile users even when traditional cookies are not used in in-app mobile inventory.[155] Defendant has engineered ways to track and target users irrespective of where that user finds themselves or what type of device they use.

158. In sum, Defendant offers a suit of products that rely on the collection of mass amounts of data on each individual, collected both from the Microsoft pixels and other sources, including Partner Pixels and other data brokers and allow for that data to be instantly sold in a large variety of ways with entities involved in the real-time bidding and advertising delivery. This is the core of the privacy violations alleged herein: not only are individuals tracked everywhere they go online, but the data collected is sold to dozens or hundreds of other parties without their consent.

[151] *Microsoft Curate – Partner Center Guide*, Microsoft (Feb. 22, 2024), https://learn.microsoft.com/en-us/xandr/curate/partner-center-guide.

[152] *Id.*

[153] *Microsoft Curate – Daypart Targeting*, Microsoft (Nov. 24, 2024), https://learn.microsoft.com/en-us/xandr/curate/daypart-targeting.

[154] *Microsoft Curate – System Targeting*, Microsoft (Jan. 29, 2025), https://learn.microsoft.com/en-us/xandr/curate/system-targeting.

[155] *Id.*

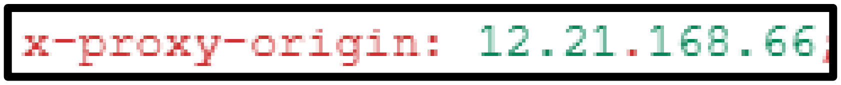
III. DEFENDANT'S PIXELS ARE PRESENT ON EACH OF THE SUBJECT WEBSITES

A. Ali Express

159. AliExpress is a discount shopping website that offers a wide variety of consumer goods for sale at very low prices.

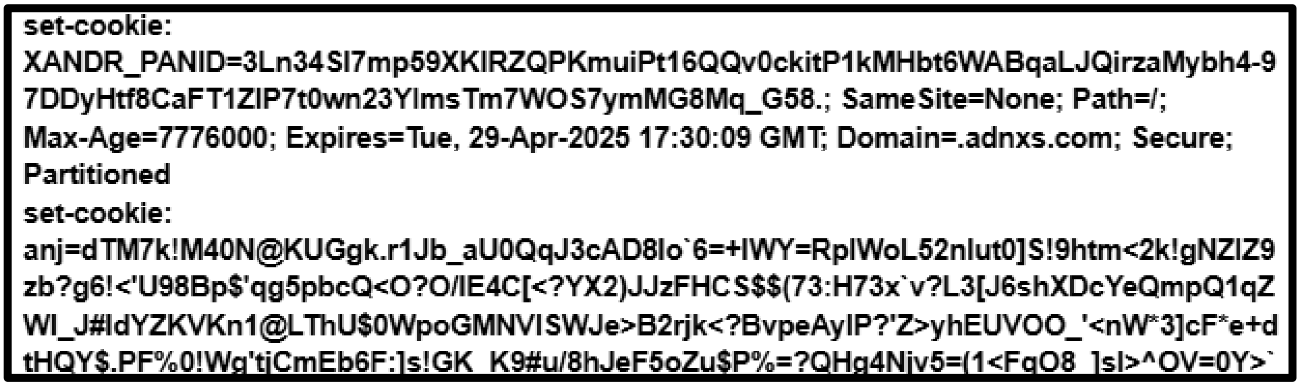
160. Unbeknownst to website visitors, the Adnxs Pixel is loaded onto the AliExpress website.

161. As soon as the individual reaches the AliExpress website, the Adnxs Pixel collects the individual's IP address.



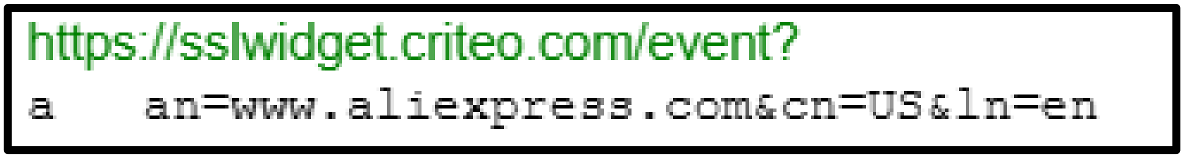
```
x-proxy-origin: 12.21.168.66;
```

162. The Adnxs Pixel also immediately loads the Adnxs Tracking Cookies onto the individual's browser in the manner described above.



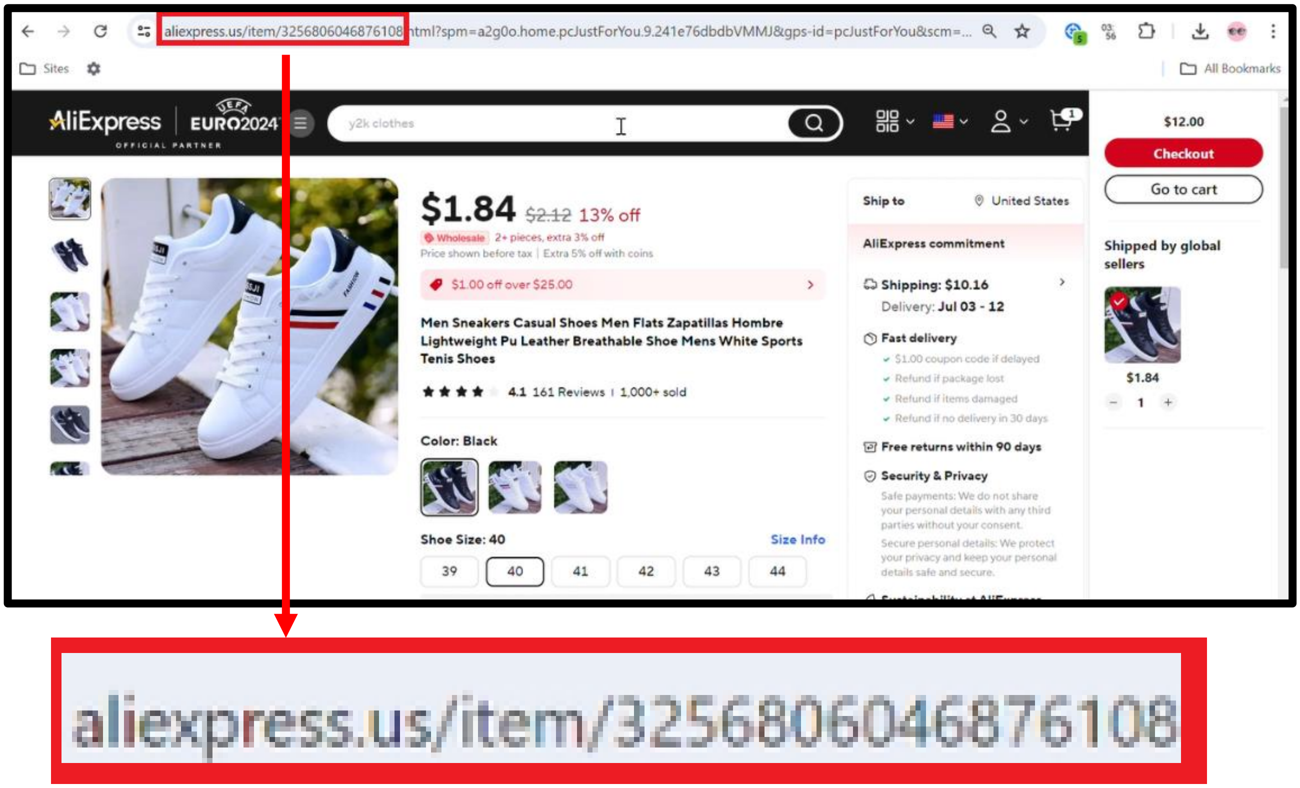
```
set-cookie:
XANDR_PANID=3Ln34SI7mp59XKIRZQPKmuiPt16QQv0ckitP1kMHbt6WABqaLJQirzaMybh4-9
7DDyHtf8CaFT1ZIP7t0wn23YlmsTm7WOS7ymMG8Mq_G58.; SameSite=None; Path=/;
Max-Age=7776000; Expires=Tue, 29-Apr-2025 17:30:09 GMT; Domain=.adnxs.com; Secure;
Partitioned
set-cookie:
anj=dTM7k!M40N@KUGgk.r1Jb_aU0QqJ3cAD8lo`6=+IWY=RplWoL52nlut0]S!9htm<2k!gNZIZ9
zb?g6!<'U98Bp$'qg5pbcQ<O?O/IE4C[<?YX2)JJzFHCS$$(73:H73x`v?L3[J6shXDcYeQmpQ1qZ
WI_J#IdYZKVKn1@LThU$0WpoGMNVISWJe>B2rjk<?BvpeAyIP?'Z>yhEUVOO_'<nW*3]cF*e+d
tHQY$.PF%0!Wg'tjCmEb6F:]s!GK_K9#u/8hJeF5oZu$P%=?QHg4Njv5=(1<FqO8_]sl>^OV=0Y>`
```

163. Also unbeknownst to visitors to the AliExpress website, the Criteo Pixel, a Partner Pixel, is loaded on the AliExpress website.



```
https://sslwidget.criteo.com/event?
a    an=www.aliexpress.com&cn=US&ln=en
```

164. When a user clicks on a particular item to view or purchase, the unique item number of that item is contained in the detailed descriptive URL of the page of the AliExpress website selling that item.


aliexpress.us/item/3256806046876108.html?spm=a2g0o.home.pcJustForYou.9.241e76dbdbVMMJ&gps-id=pcJustForYou&scm=...
Sites
All Bookmarks
AliExpress
EURO2024
OFFICIAL PARTNER
y2k clothes
$12.00
Checkout
Go to cart
Shipped by global sellers
$1.84
1
Color: Black
Shoe Size: 40
Size Info
39
40
41
42
43
44
aliexpress.us/item/3256806046876108

$1.84 ~~$2.12~~ 13% off

Wholesale 2+ pieces, extra 3% off

Price shown before tax | Extra 5% off with coins

$1.00 off over $25.00

Men Sneakers Casual Shoes Men Flats Zapatillas Hombre Lightweight Pu Leather Breathable Shoe Mens White Sports Tenis Shoes

★★★★ 4.1 161 Reviews | 1,000+ sold

Ship to United States

AliExpress commitment

Shipping: $10.16
Delivery: Jul 03 - 12

Fast delivery
- $1.00 coupon code if delayed
- Refund if package lost
- Refund if items damaged
- Refund if no delivery in 30 days

Free returns within 90 days

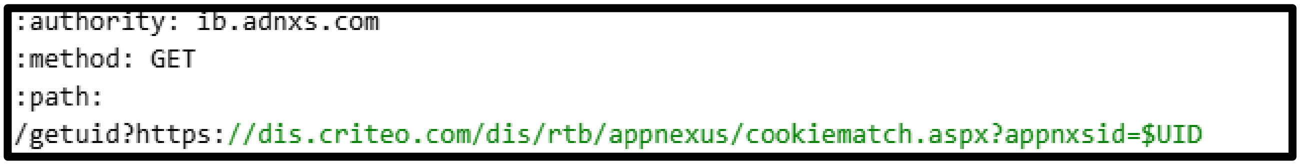
Security & Privacy
Safe payments: We do not share your personal details with any third parties without your consent.
Secure personal details: We protect your privacy and keep your personal details safe and secure.

165. As the information is entered into the website (i.e., in real time) the Criteo Pixel intercepts the information by receiving the page URL in a "GET request."

```
tld aliexpress.us
fu
https://www.aliexpress.us/item/3256806046876108.html?spm=a2g0o.home.pcJustForYou.9
.241e76dbdbVMMJ&gps-id=pcJustForYou&scm=1007.13562.333647.0&scm_id=1007.13562.3336
47.0&scm-url=1007.13562.333647.0&pvid=c0aeedc9-5d29-43e2-adb3-a1695384d3be&_t=gps-
id:pcJustForYou,scm-url:1007.13562.333647.0,pvid:c0aeedc9-5d29-43e2-adb3-a1695384d
3be,tpp_buckets:668%232846%238115%232000&pdp_npi=4%40dis%21USD%212.12%211.84%21%21
%212.12%211.84%21%402101fb0c17193452861613171ea95c%2112000036393276923%21rec%21US%
21%21AB&utparam-url=scene%3ApcJustForYou%7Cquery_from%3A
```

166. Xandr, through the Adnxs Pixel, provides identity resolution to a number of Partner Pixels on the AliExpress website.

167. Specifically, Adnxs shares the unique user ID and profile information with Criteo and a number of currently unknown Partner Pixels. The phrase "cookiematch" indicates identity resolution and "rtb" indicates the information is used in the real-time bidding process.

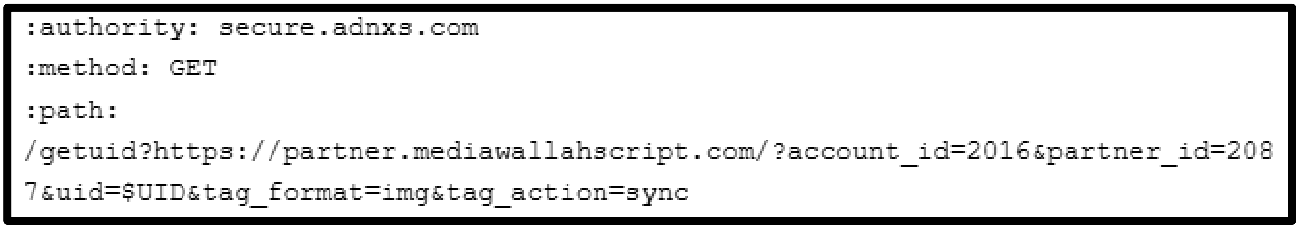


```
:authority: ib.adnxs.com
:method: GET
:path:
/getuid?https://dis.criteo.com/dis/rtb/appnexus/cookiematch.aspx?appnxsid=$UID
```

168. Receiving the UID allows Criteo and any other Partner Pixel to identify which individual is entering which information into the AliExpress website and, thus the Adnxs Pixel aids Criteo's wiretapping.

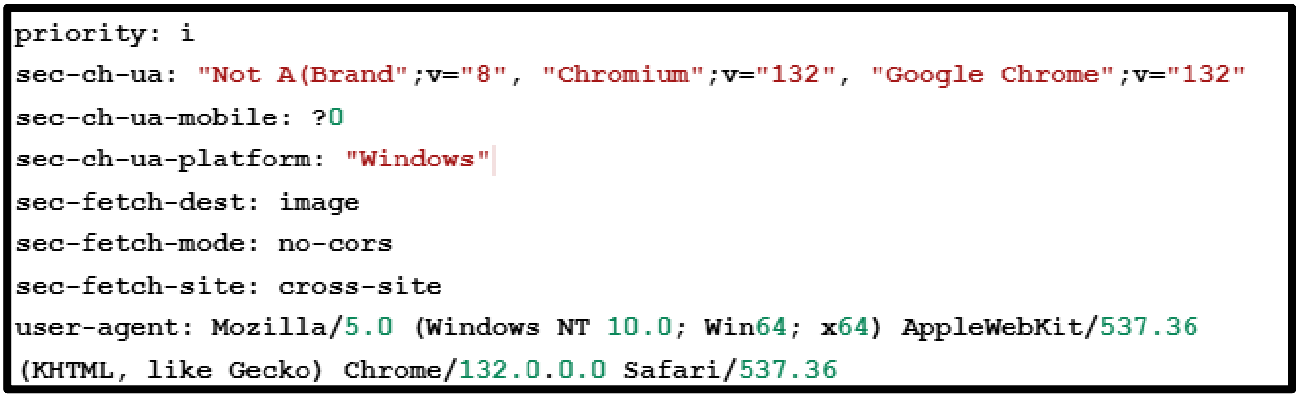
169. Further, the Adnxs Pixel works with other providers of identity resolution on the AliExpress website to bolster its own profile of an individual.

170. Plaintiffs' testing shows the Adnxs Pixel working with a number of Partner Pixels, including the MediaWallah Pixel, to obtain identity resolution. This additional information is then added to Defendant's consumer and advertising profiles.



```
:authority: secure.adnxs.com
:method: GET
:path:
/getuid?https://partner.mediawallahscript.com/?account_id=2016&partner_id=208
7&uid=$UID&tag_format=img&tag_action=sync
```

171. The Adnxs Pixel also collects user device information as described above.



```
priority: i
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
```

172. 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

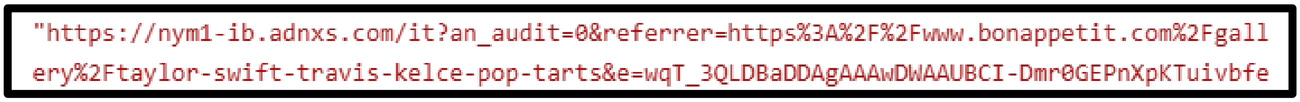
to its consumer profiles and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

B. Bon Appetit

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

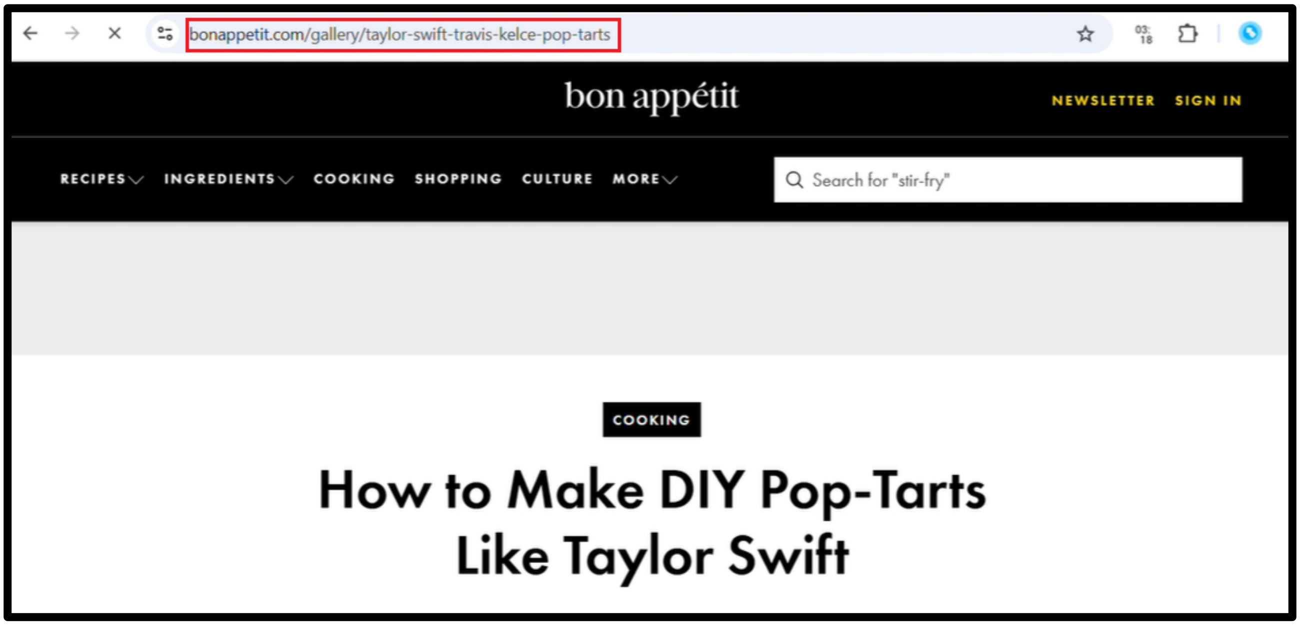
174. The website also contains ad space where companies, like Defendant, act as an advertising exchange and facilitate the real-time bidding process to hyper-target advertisements to individual website users based on data collected about their browsing activity and other activity.

175. Unbeknownst to website visitors, the Adnxs Pixel is loaded onto the Bon Appetit website.



```
"https://nym1-ib.adnxs.com/it?an_audit=0&referrer=https%3A%2F%2Fwww.bonappetit.com%2Fgall
ery%2Ftaylor-swift-travis-kelce-pop-tarts&e=wqT_3QLDBaDDAgAAAwDWAAUBCI-Dmr0GEPnXpKTuivbfe
```

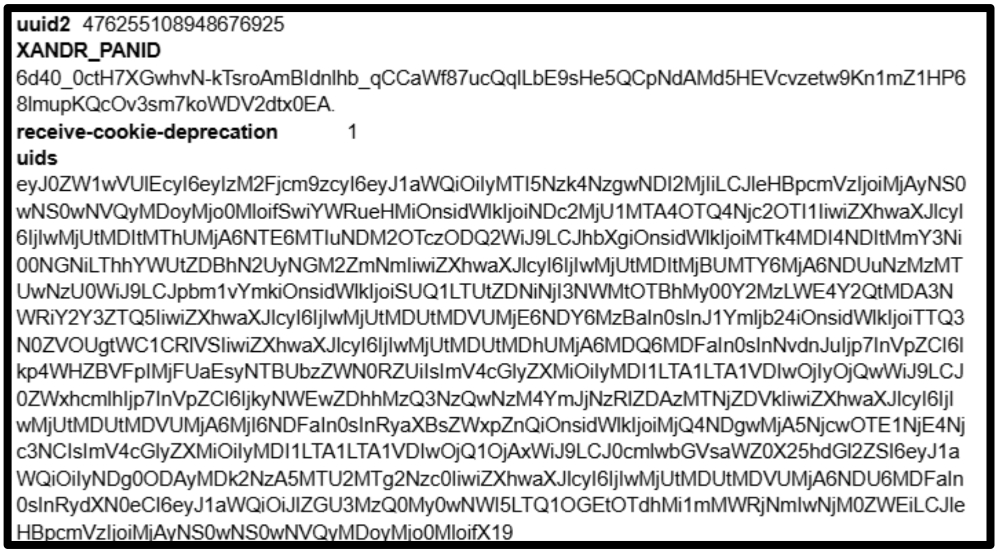
176. As shown above, the Adnxs Pixel collects the detailed descriptive URL of the specific articles viewed by each website visitor and the articles are selected on the website (i.e., in real time), and thus collects the affirmative selections of articles by each visitor to the Bon Appetit website.



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

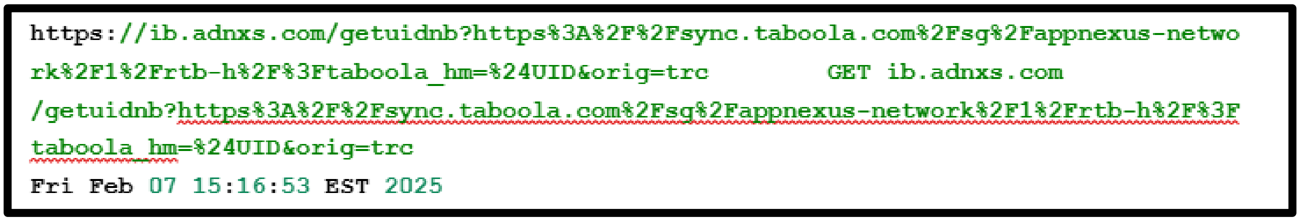
177. As soon as the individual user reaches the Bon Appetit website, the Adnxs Pixel collects the user's IP address.

178. The Adnxs Pixel also immediately loads the Adnxs Tracking Cookies onto the individual's browser in the manner described above.

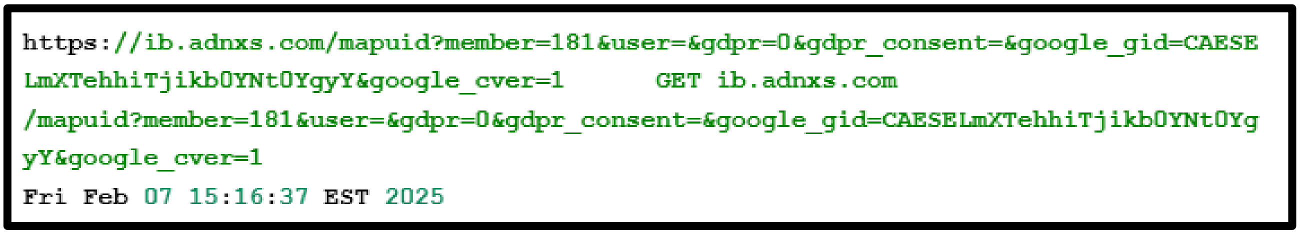


```
uuid2  476255108948676925
XANDR_PANID
6d40_0ctH7XGwhvN-kTsroAmBIdnlhb_qCCaWf87ucQqlLbE9sHe5QCpNdAMd5HEVcvzetw9Kn1mZ1HP6
8lmupKQcOv3sm7koWDV2dtx0EA.
receive-cookie-deprecation        1
uids
eyJ0ZW1wVUlEcyI6eyIzM2Fjcm9zcyI6eyJ1aWQiOiIyMTI5Nzk4NzgwNDI2MjliLCJleHBpcmVzIjoiMjAyNS0
wNS0wNVQyMDoyMjo0MloifSwiYWRueHMiOnsidWlkIjoiNDc2MjU1MTA4OTQ4Njc2OTI1IiwiZXhwaXJlcyI
6IjIwMjUtMDItMThUMjA6NTE6MTIuNDM2OTczODQ2WiJ9LCJhbXgiOnsidWlkIjoiMTk4MDI4NDItMmY3Ni
00NGNiLThhYWUtZDBhN2UyNGM2ZmNmIiwiZXhwaXJlcyI6IjIwMjUtMDItMjBUMTY6MjA6NDUuNzMzMT
UwNzU0WiJ9LCJpbm1vYmkiOnsidWlkIjoiSUQ1LTUtZDNiNjI3NWMtOTBhMy00Y2MzLWE4Y2QtMDA3N
WRiY2Y3ZTQ5IiwiZXhwaXJlcyI6IjIwMjUtMDUtMDVUMjE6NDY6MzBaIn0sInJ1Ymljb24iOnsidWlkIjoiTTQ3
N0ZVOUgtWC1CRlVSIiwiZXhwaXJlcyI6IjIwMjUtMDUtMDhUMjA6MDQ6MDFaIn0sInNvdnJuIjp7InVpZCI6I
kp4WHZBVFpIMjFUaEsyNTBUbzZWN0RZUiIsImV4cGlyZXMiOiIyMDI1LTA1LTA1VDIwOjIyOjQwWiJ9LCJ
0ZWxhcmlhIjp7InVpZCI6IjkyNWEwZDhhMzQ3NzQwNzM4YmJjNzRlZDAzMTNjZDVkIiwiZXhwaXJlcyI6IjI
wMjUtMDUtMDVUMjA6MjI6NDFaIn0sInRyaXBsZWxpZnQiOnsidWlkIjoiMjQ4NDgwMjA5NjcwOTE1NjE4Nj
c3NCIsImV4cGlyZXMiOiIyMDI1LTA1LTA1VDIwOjQ1OjAxWiJ9LCJ0cmlwbGVsaWZ0X25hdGl2ZSI6eyJ1a
WQiOiIyNDg0ODAyMDk2NzA5MTU2MTg2Nzc0IiwiZXhwaXJlcyI6IjIwMjUtMDUtMDVUMjA6NDU6MDFaIn
0sInRydXN0eCI6eyJ1aWQiOiJlZGU3MzQ0My0wNWI5LTQ1OGEtOTdhMi1mMWRjNmIwNjM0ZWEiLCJle
HBpcmVzIjoiMjAyNS0wNS0wNVQyMDoyMjo0MloifX19
```

179. Defendant, through the Adnxs Pixel, provides identity resolution to over 20 Partner Pixels on the Bon Appetit website throught getUID, and mapUID requests.



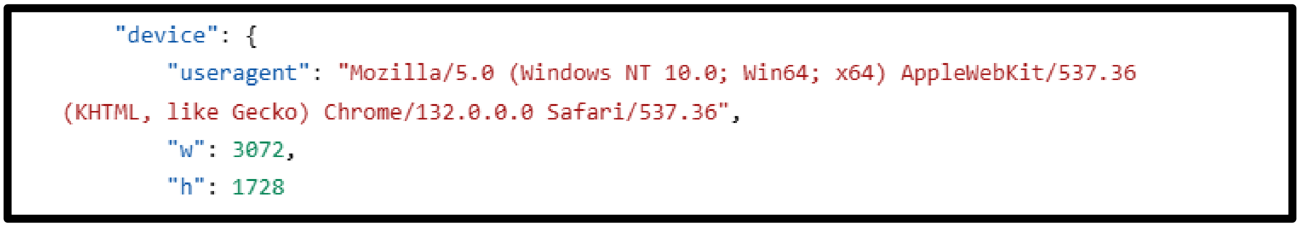
```
https://ib.adnxs.com/getuidnb?https%3A%2F%2Fsync.taboola.com%2Fsg%2Fappnexus-netwo
rk%2F1%2Frtb-h%2F%3Ftaboola_hm=%24UID&orig=trc        GET ib.adnxs.com
/getuidnb?https%3A%2F%2Fsync.taboola.com%2Fsg%2Fappnexus-network%2F1%2Frtb-h%2F%3F
taboola_hm=%24UID&orig=trc
Fri Feb 07 15:16:53 EST 2025
```



```
https://ib.adnxs.com/mapuid?member=181&user=&gdpr=0&gdpr_consent=&google_gid=CAESE
LmXTehhiTjikb0YNt0YgyY&google_cver=1       GET ib.adnxs.com
/mapuid?member=181&user=&gdpr=0&gdpr_consent=&google_gid=CAESELmXTehhiTjikb0YNt0Yg
yY&google_cver=1
Fri Feb 07 15:16:37 EST 2025
```

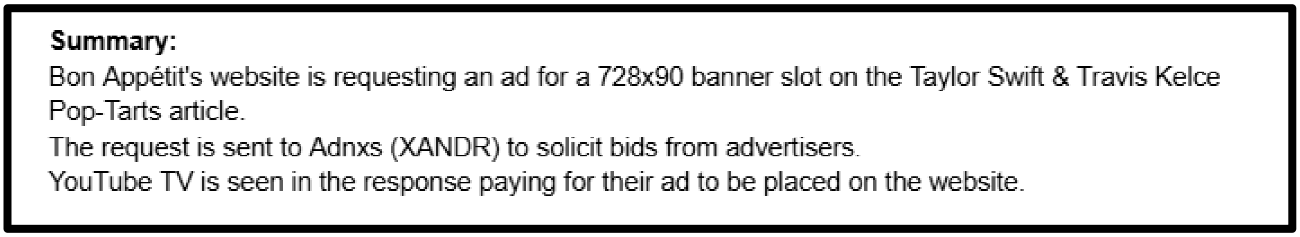
180. Further, the Adnxs Pixel works with other providers of identity resolution on the AliExpress website to bolster its own profile of each individual website user by incorporating the information gathered on an individual by those providers.

181. The Adnxs Pixel also collects each individual's device information as described above.

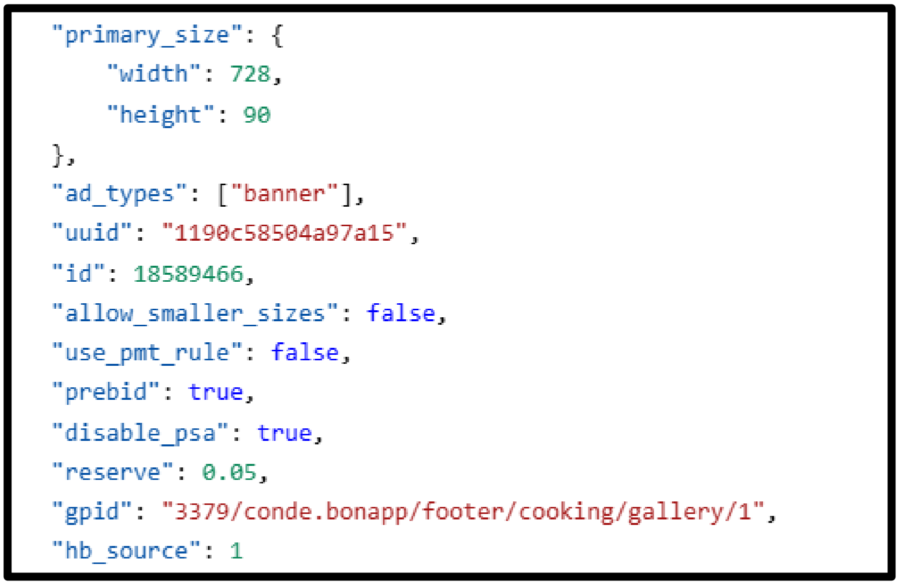


```
    "device": {
        "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36",
        "w": 3072,
        "h": 1728
```

182. Defendant also services real time bidding for advertisements on the Bon Appetit website. To do this, Defendant uses the real-time bidding process described above to auction off the ad space to advertisers interested in reaching the particular user, who is identified and profiled by Xandr and the Adnxs Pixel. Plaintiffs' testing showed Xandr soliciting bids for a banner advertisement on the selected page. YouTube TV (through Google's advertising service, DoubleClick) won the auction and paid approximately a $0.67 cost per thousand impressions ("CPM") to run the advertisement.[156]

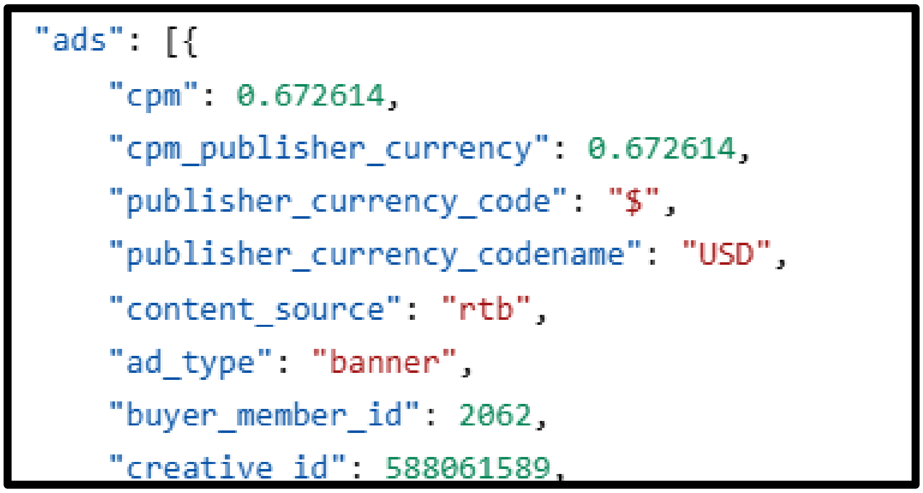


Summary:
Bon Appétit's website is requesting an ad for a 728x90 banner slot on the Taylor Swift & Travis Kelce Pop-Tarts article.
The request is sent to Adnxs (XANDR) to solicit bids from advertisers.
YouTube TV is seen in the response paying for their ad to be placed on the website.

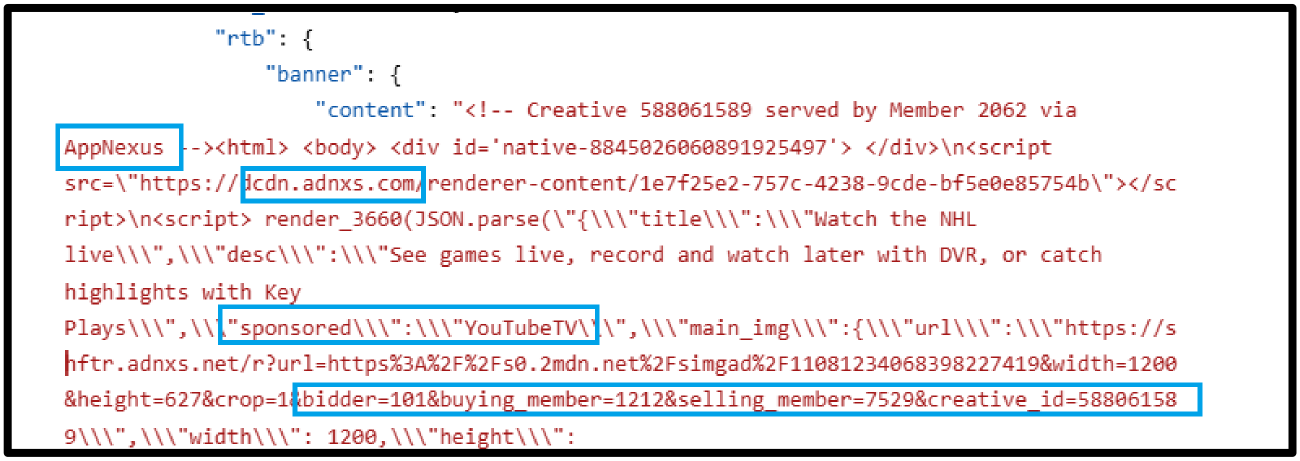


```
"primary_size": {
    "width": 728,
    "height": 90
},
"ad_types": ["banner"],
"uuid": "1190c58504a97a15",
"id": 18589466,
"allow_smaller_sizes": false,
"use_pmt_rule": false,
"prebid": true,
"disable_psa": true,
"reserve": 0.05,
"gpid": "3379/conde.bonapp/footer/cooking/gallery/1",
"hb_source": 1
```

[156] https://www.criteo.com/wp-content/uploads/2017/07/Report-criteo-the-smart-marketers-guide-to-retargeting-acronyms-one-pager.pdf



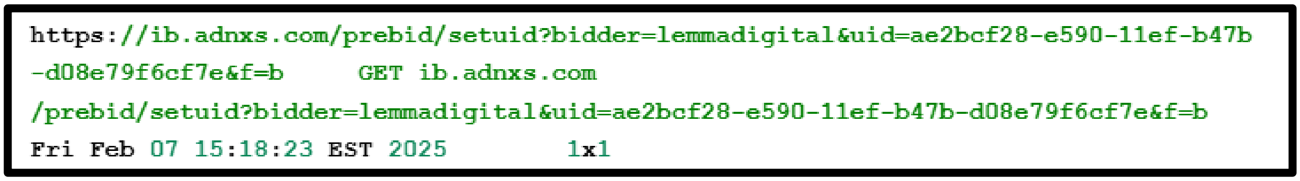
```
"ads": [{
    "cpm": 0.672614,
    "cpm_publisher_currency": 0.672614,
    "publisher_currency_code": "$",
    "publisher_currency_codename": "USD",
    "content_source": "rtb",
    "ad_type": "banner",
    "buyer_member_id": 2062,
    "creative_id": 588061589,
```



```
            "rtb": {
                "banner": {
                    "content": "<!-- Creative 588061589 served by Member 2062 via
AppNexus --><html> <body> <div id='native-8845026060891925497'> </div>\n<script
src=\"https://cdn.adnxs.com/renderer-content/1e7f25e2-757c-4238-9cde-bf5e0e85754b\"></sc
ript>\n<script> render_3660(JSON.parse(\"{\\\"title\\\":\\\"Watch the NHL
live\\\",\\\"desc\\\":\\\"See games live, record and watch later with DVR, or catch
highlights with Key
Plays\\\",\\\"sponsored\\\":\\\"YouTubeTV\\\",\\\"main_img\\\":{\\\"url\\\":\\\"https://s
hftr.adnxs.net/r?url=https%3A%2F%2Fs0.2mdn.net%2Fsimgad%2F11081234068398227419&width=1200
&height=627&crop=1&bidder=101&buying_member=1212&selling_member=7529&creative_id=58806158
9\\\",\\\"width\\\": 1200,\\\"height\\\":
```

183. 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.

184. Plaintiffs' testing showed dozens of "prebid" requests related to the ad space facilitated by Defendant, meaning the individual website user's information is shared with each of those companies.



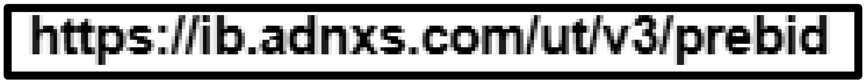
```
https://ib.adnxs.com/prebid/setuid?bidder=lemmadigital&uid=ae2bcf28-e590-11ef-b47b
-d08e79f6cf7e&f=b      GET ib.adnxs.com
/prebid/setuid?bidder=lemmadigital&uid=ae2bcf28-e590-11ef-b47b-d08e79f6cf7e&f=b
Fri Feb 07 15:18:23 EST 2025         1x1
```

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

C. Buzzfeed

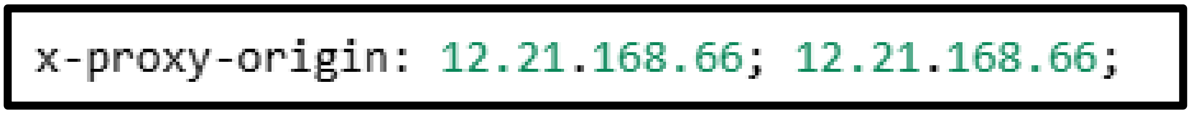
186. Buzzfeed is a popular entertainment and culture website, featuring a variety of articles and quizzes related to popular culture.

187. Unbeknownst to visitors of the Buzzfeed website, the Adnxs Pixel is loaded onto the website.



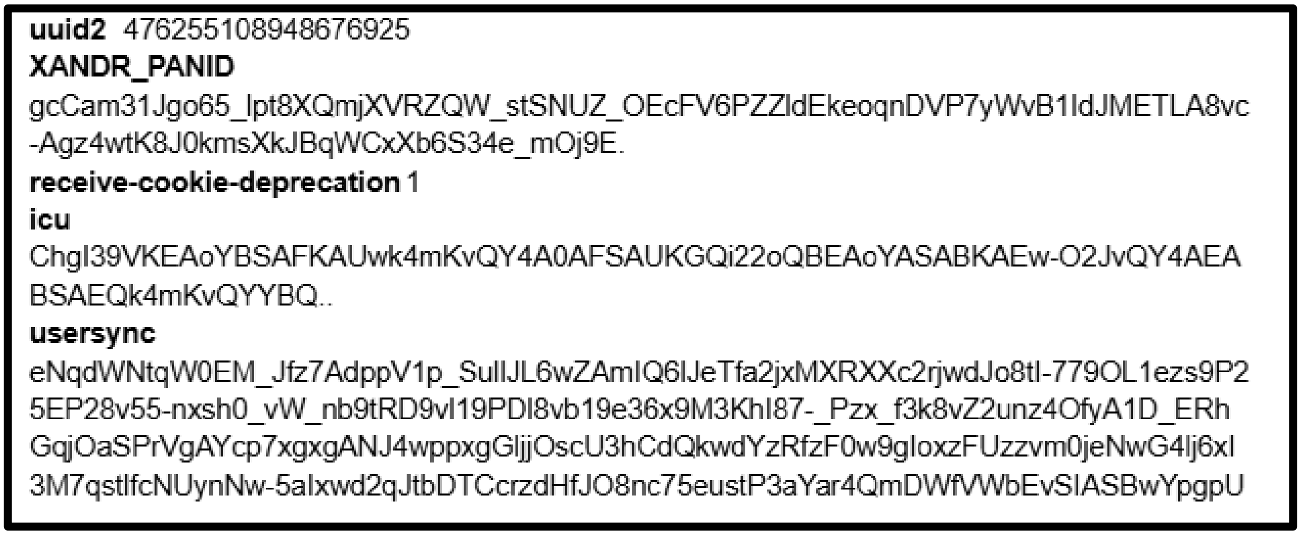
```
https://ib.adnxs.com/ut/v3/prebid
```

188. When a user visits the Buzzfeed website, the Adnxs Pixel automatically collects the user's IP address.



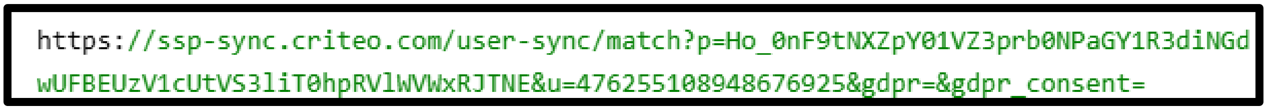
```
x-proxy-origin: 12.21.168.66; 12.21.168.66;
```

189. The Adnxs Pixel also immediately loads the Adnxs Tracking Cookies onto the individual's browser in the manner described above.



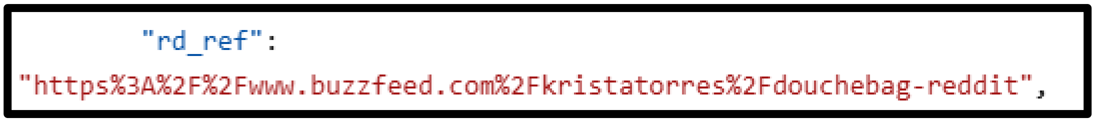
```
uuid2 476255108948676925
XANDR_PANID
gcCam31Jgo65_lpt8XQmjXVRZQW_stSNUZ_OEcFV6PZZldEkeoqnDVP7yWvB1IdJMETLA8vc
-Agz4wtK8J0kmsXkJBqWCxXb6S34e_mOj9E.
receive-cookie-deprecation 1
icu
ChgI39VKEAoYBSAFKAUwk4mKvQY4A0AFSAUKGQi22oQBEAoYASABKAEw-O2JvQY4AEA
BSAEQk4mKvQYYBQ..
usersync
eNqdWNtqW0EM_Jfz7AdppV1p_SulIJL6wZAmIQ6lJeTfa2jxMXRXXc2rjwdJo8tl-779OL1ezs9P2
5EP28v55-nxsh0_vW_nb9tRD9vl19PDl8vb19e36x9M3KhI87-_Pzx_f3k8vZ2unz4OfyA1D_ERh
GqjOaSPrVgAYcp7xgxgANJ4wppxgGljjOscU3hCdQkwdYzRfzF0w9gloxzFUzzvm0jeNwG4lj6xl
3M7qstlfcNUynNw-5alxwd2qJtbDTCcrzdHfJO8nc75eustP3aYar4QmDWfVWbEvSIASBwYpgpU
```

190. Defendant provides identity resolution to *at least 11 Partner Pixels on the Buzzfeed website*. The Adnxs Pixel shares both the UID created to track users with the cookies loaded onto their browsers and the user's IP address with each Partner Pixel.



```
https://ssp-sync.criteo.com/user-sync/match?p=Ho_0nF9tNXZpY01VZ3prb0NPaGY1R3diNGd
wUFBEUzV1cUtVS3liT0hpRVlWVWxRJTNE&u=4762551089486769258&gdpr=&gdpr_consent=
```

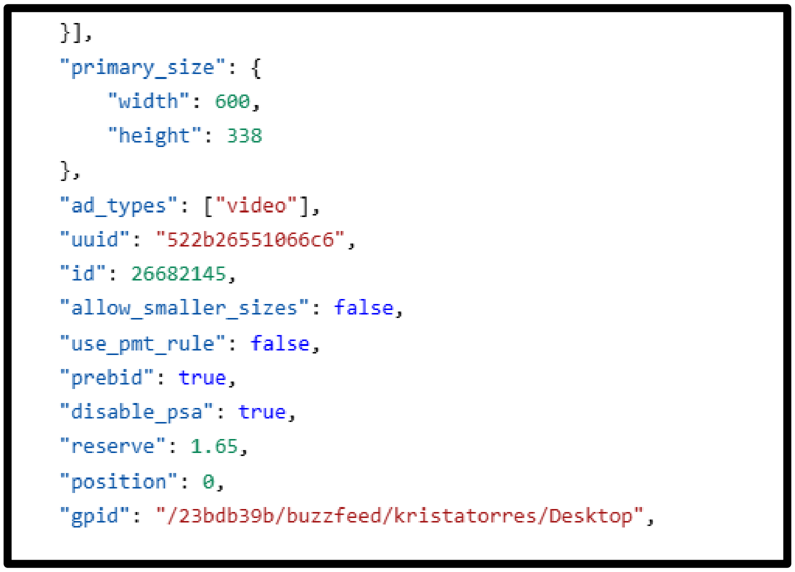
191. Defendant also services real time bidding for advertisements on the Buzzfeed website. To do this, Defendant identifies the user as described above and collects the URL for the page visited by the user as the user clicks on a particular link or article (i.e., in real time).



```
          "rd_ref":
"https%3A%2F%2Fwww.buzzfeed.com%2Fkristatorres%2Fdouchebag-reddit",
```

192. Defendant also shares the information it has gathered on a particular user through its Microsoft Invest, Microsoft Monetize, and Microsoft Curate products to allow bidding partners to know that their advertisements will be targeted to a user's interests.

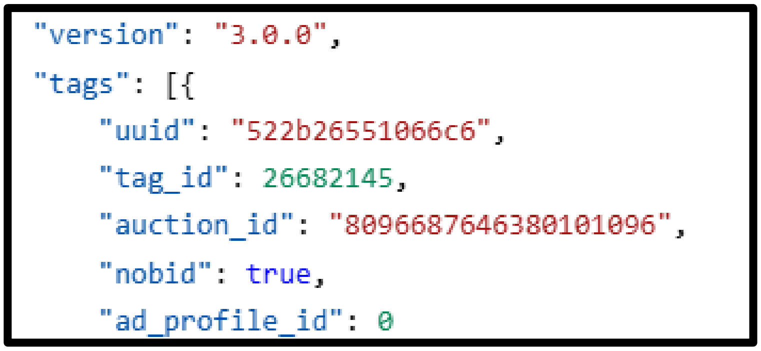
193. Defendant facilitates advertising on specific spaces on the Buzzfeed website. For example, Xandr operates the advertising space for a video ad on a particular article published by Buzzfeed.



```
}],
"primary_size": {
    "width": 600,
    "height": 338
},
"ad_types": ["video"],
"uuid": "522b26551066c6",
"id": 26682145,
"allow_smaller_sizes": false,
"use_pmt_rule": false,
"prebid": true,
"disable_psa": true,
"reserve": 1.65,
"position": 0,
"gpid": "/23bdb39b/buzzfeed/kristatorres/Desktop",
```

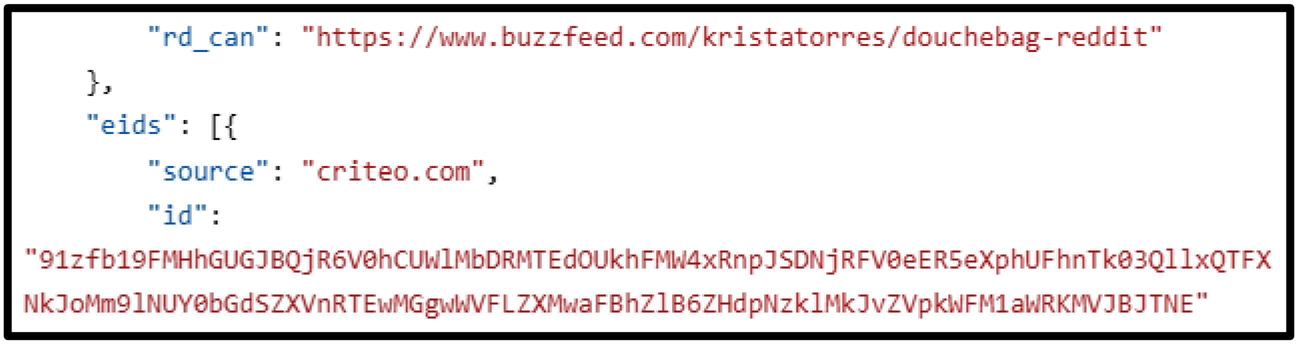
194. Defendant uses the real-time bidding process described above to auction off the ad space to advertisers interested in reaching the particular user, who is identified and profiled by

Defendant and the Adnxs Pixel. In the image below, the auction id shows that the ad space is available for bidding and the UUID is the unique identifier assigned to a particular user.



```
"version": "3.0.0",
"tags": [{
    "uuid": "522b26551066c6",
    "tag_id": 26682145,
    "auction_id": "8096687646380101096",
    "nobid": true,
    "ad_profile_id": 0
```

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



```
        "rd_can": "https://www.buzzfeed.com/kristatorres/douchebag-reddit"
    },
    "eids": [{
        "source": "criteo.com",
        "id":
"91zfb19FMHhGUGJBQjR6V0hCUWlMbDRMTEdOUkhFMW4xRnpJSDNjRFV0eER5eXphUFhnTk03QllxQTFX
NkJoMm9lNUY0bGdSZXVnRTEwMGgwWVFLZXMwaFBhZlB6ZHdpNzklMkJvZVpkWFM1aWRKMVJBJTNE"
```

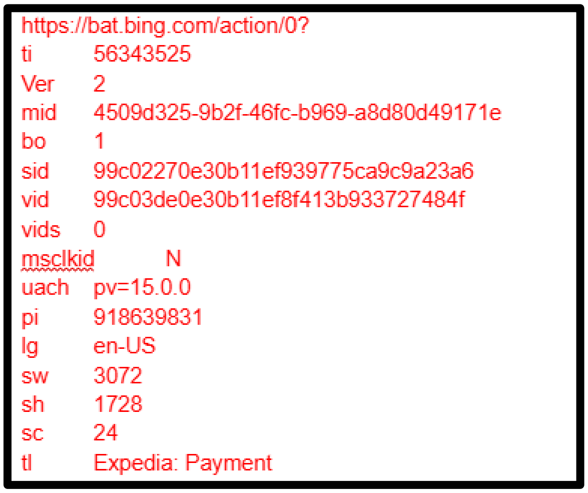
196. As with the Bon Appetit website, the facilitation of advertising space requires the sharing of information about each user with multiple parties who may bid to advertise to that particular user.

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

D. Expedia

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

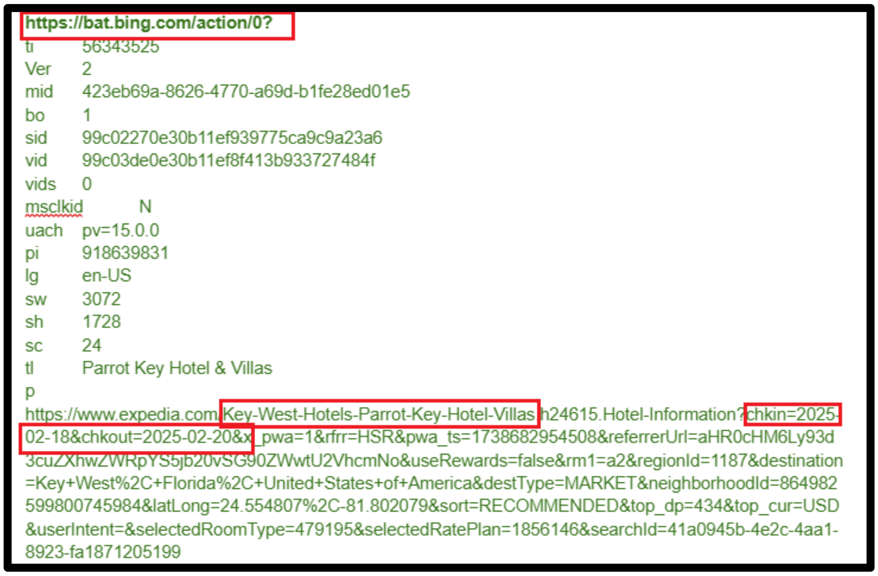
199. Unbeknownst to website visitors, the Bing Pixel is loaded onto the Expedia website.



```
https://bat.bing.com/action/0?
ti       56343525
Ver      2
mid      4509d325-9b2f-46fc-b969-a8d80d49171e
bo       1
sid      99c02270e30b11ef939775ca9c9a23a6
vid      99c03de0e30b11ef8f413b933727484f
vids     0
msclkid          N
uach     pv=15.0.0
pi       918639831
lg       en-US
sw       3072
sh       1728
sc       24
tl       Expedia: Payment
```

200. When a user clicks on a particular reservation—and again when they complete the purchase, the name of the hotel and dates of booking are contained in the detailed descriptive URL of each page as described above.

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



```
https://bat.bing.com/action/0?
ti       56343525
Ver      2
mid      423eb69a-8626-4770-a69d-b1fe28ed01e5
bo       1
sid      99c02270e30b11ef939775ca9c9a23a6
vid      99c03de0e30b11ef8f413b933727484f
vids     0
msclkid          N
uach     pv=15.0.0
pi       918639831
lg       en-US
sw       3072
sh       1728
sc       24
tl       Parrot Key Hotel & Villas
p
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=aHR0cHM6Ly93d
3cuZXhwZWRpYS5jb20vSG90ZWwtU2VhcmNo&useRewards=false&rm1=a2&regionId=1187&destination
=Key+West%2C+Florida%2C+United+States+of+America&destType=MARKET&neighborhoodId=864982
599800745984&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
```

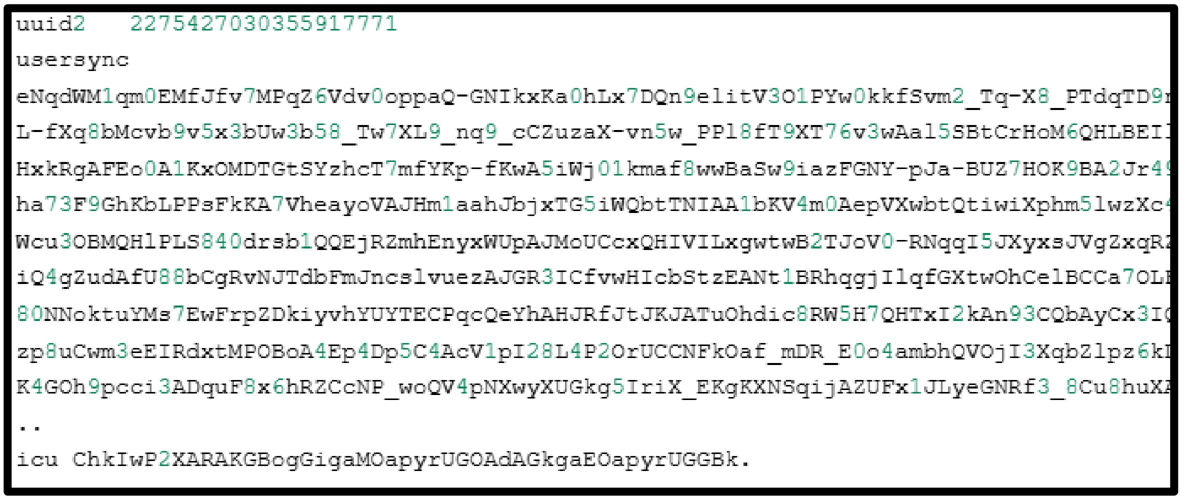
202. The information collected by the Bing Pixel is then transferred to Defendant, who adds it to its consumer profiles, which are included in the products described above and used in the real-time-bidding process.

E. Hyatt

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

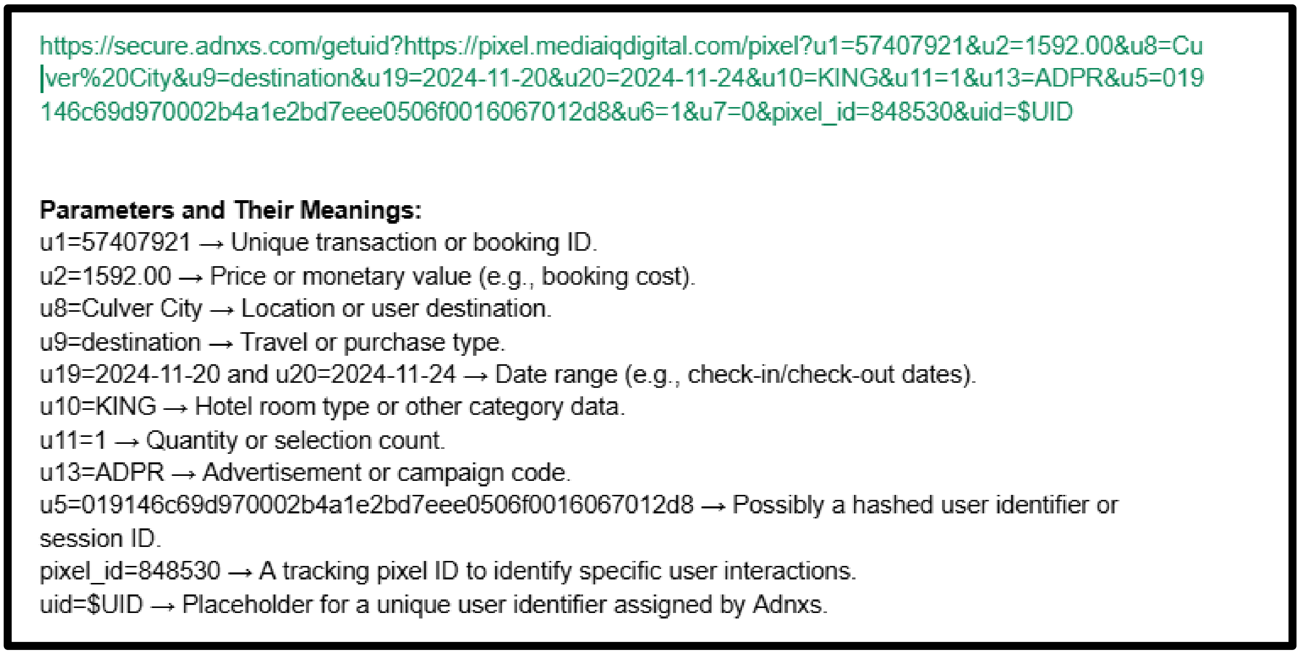
204. Unbeknownst to website visitors, the Adnxs Pixel is loaded onto the Hyatt website.

205. The Adnxs Pixel immediately loads the Adnxs Tracking Cookies onto the individual's browser in the manner described above.



```
uuid2   2275427030355917771
usersync
eNqdWM1qm0EMfJfv7MPqZ6Vdv0oppaQ-GNIkxKa0hLx7DQn9elitV3O1PYw0kkfSvm2_Tq-X8_PTdqTD9
L-fXq8bMcvb9v5x3bUw3b58_Tw7XL9_nq9_cCZuzaX-vn5w_PPl8fT9XT76v3wAal5SBtCrHoM6QHLBEI
HxkRgAFEo0A1KxOMDTGtSYzhcT7mfYKp-fKwA5iWj01kmaf8wwBaSw9iazFGNY-pJa-BUZ7HOK9BA2Jr4
ha73F9GhKbLPPsFkKA7VheayoVAJHm1aahJbjxTG5iWQbtTNIAA1bKV4m0AepVXwbtQtiwiXphm5lwzXc
Wcu3OBMQHlPLS840drsb1QQEjRZmhEnyxWUpAJMoUCcxQHIVILxgwtwB2TJoV0-RNqqI5JXyxsJVgZxqR
iQ4gZudAfU88bCgRvNJTdbFmJncslvuezAJGR3ICfvwHIcbStzEANt1BRhqgjIlqfGXtwOhCelBCCa7OL
80NNoktuYMs7EwFrpZDkiyvhYUYTECPqcQeYhAHJRfJtJKJATuOhdic8RW5H7QHTxI2kAn93CQbAyCx3I
zp8uCwm3eEIRdxtMPOBoA4Ep4Dp5C4AcV1pI28L4P2OrUCCNFkOaf_mDR_E0o4ambhQVOjI3XqbZlpz6k
K4GOh9pcci3ADquF8x6hRZCcNP_woQV4pNXwyXUGkg5IriX_EKgKXNSqijAZUFx1JLyeGNRf3_8Cu8huX
..
icu ChkIwP2XARAKGBogGigaMOapyrUGOAdAGkgaEOapyrUGGBk.
```

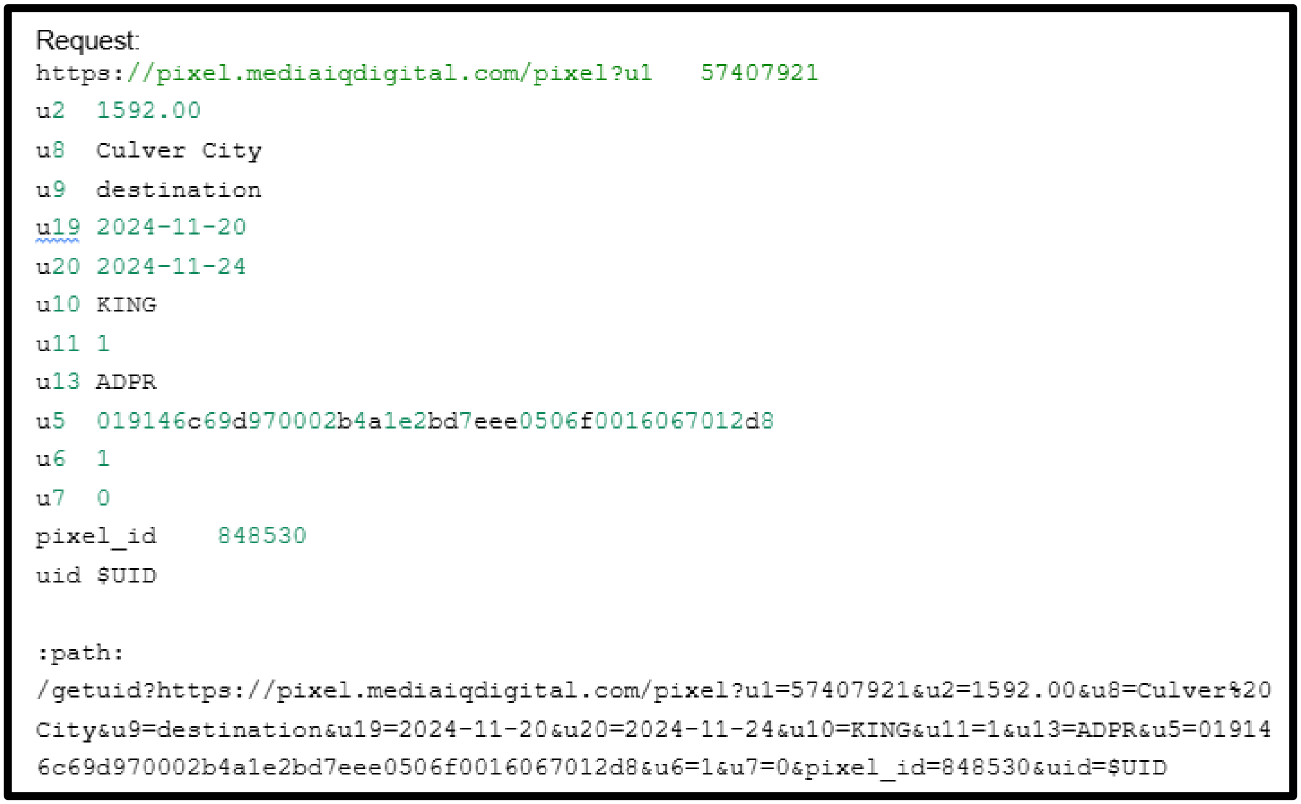
206. As website visitors select hotels and dates of booking (i.e. in real time), the Adnxs Pixel intercepts this information.



```
https://secure.adnxs.com/getuid?https://pixel.mediaiqdigital.com/pixel?u1=57407921&u2=1592.00&u8=Cu
ver%20City&u9=destination&u19=2024-11-20&u20=2024-11-24&u10=KING&u11=1&u13=ADPR&u5=019
146c69d970002b4a1e2bd7eee0506f0016067012d8&u6=1&u7=0&pixel_id=848530&uid=$UID
```

Parameters and Their Meanings:
u1=57407921 → Unique transaction or booking ID.
u2=1592.00 → Price or monetary value (e.g., booking cost).
u8=Culver City → Location or user destination.
u9=destination → Travel or purchase type.
u19=2024-11-20 and u20=2024-11-24 → Date range (e.g., check-in/check-out dates).
u10=KING → Hotel room type or other category data.
u11=1 → Quantity or selection count.
u13=ADPR → Advertisement or campaign code.
u5=019146c69d970002b4a1e2bd7eee0506f0016067012d8 → Possibly a hashed user identifier or session ID.
pixel_id=848530 → A tracking pixel ID to identify specific user interactions.
uid=$UID → Placeholder for a unique user identifier assigned by Adnxs.

207. The Adnxs Pixel also shares the intercepted information with Partner Pixels. The below image shows the Adnxs Pixel passing the individual's UID, alongside the intercepted information, to Media IQ (now known as MIQ), another data broker who uses intercepted information to service advertising.



```
Request:
https://pixel.mediaiqdigital.com/pixel?u1    57407921
u2  1592.00
u8  Culver City
u9  destination
u19 2024-11-20
u20 2024-11-24
u10 KING
u11 1
u13 ADPR
u5  019146c69d970002b4a1e2bd7eee0506f0016067012d8
u6  1
u7  0
pixel_id    848530
uid $UID

:path:
/getuid?https://pixel.mediaiqdigital.com/pixel?u1=57407921&u2=1592.00&u8=Culver%20
City&u9=destination&u19=2024-11-20&u20=2024-11-24&u10=KING&u11=1&u13=ADPR&u5=01914
6c69d970002b4a1e2bd7eee0506f0016067012d8&u6=1&u7=0&pixel_id=848530&uid=$UID
```

208. The Adnxs Pixel provides similar identity resolution to at least 2 other Partner Pixels.

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

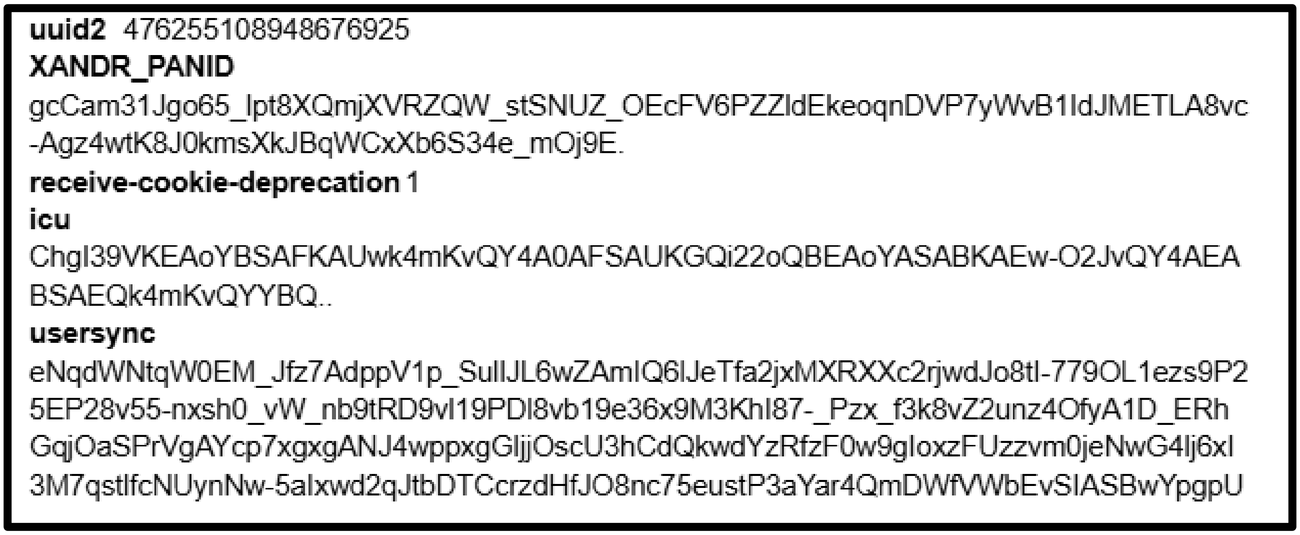
F. Plushcare

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

211. Unbeknownst to website visitors, the Adnxs Pixel is loaded onto the Plushcare Website.

212. When a user visits the Plushcare website, the Adnxs Pixel automatically collects the user's IP address.

213. The Adnxs Pixel also immediately loads the Adnxs Tracking Cookies onto the individual's browser in the manner described above.



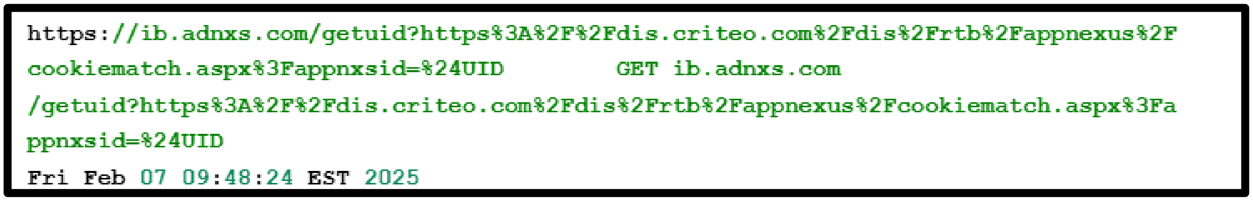
```
uuid2 476255108948676925
XANDR_PANID
gcCam31Jgo65_lpt8XQmjXVRZQW_stSNUZ_OEcFV6PZZldEkeoqnDVP7yWvB1ldJMETLA8vc
-Agz4wtK8J0kmsXkJBqWCxXb6S34e_mOj9E.
receive-cookie-deprecation 1
icu
ChgI39VKEAoYBSAFKAUwk4mKvQY4A0AFSAUKGQi22oQBEAoYASABKAEw-O2JvQY4AEA
BSAEQk4mKvQYYBQ..
usersync
eNqdWNtqW0EM_Jfz7AdppV1p_SulIJL6wZAmIQ6lJeTfa2jxMXRXXc2rjwdJo8tl-779OL1ezs9P2
5EP28v55-nxsh0_vW_nb9tRD9vl19PDl8vb19e36x9M3KhI87-_Pzx_f3k8vZ2unz4OfyA1D_ERh
GqjOaSPrVgAYcp7xgxgANJ4wppxgGljjOscU3hCdQkwdYzRfzF0w9gloxzFUzzvm0jeNwG4lj6xl
3M7qstlfcNUynNw-5alxwd2qJtbDTCcrzdHfJO8nc75eustP3aYar4QmDWfVWbEvSIASBwYpgpU
```

214. 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.

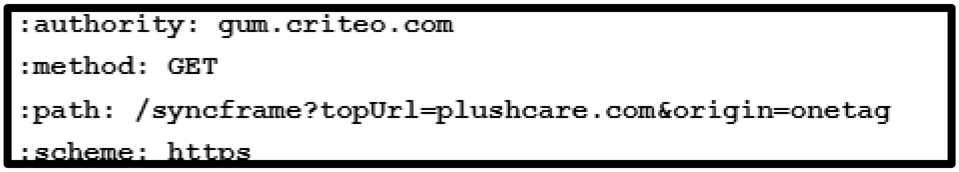
215. Defendant also provides identity resolution to <u>at least 3 Partner Pixels, including the Criteo Pixel on the Plushcare website.</u> The Adnxs Pixel shares both the UID created to track users with the cookies loaded onto their browsers and the user's IP address with each Partner Pixel

216. Unbeknownst to visitors on the Plushcare website, the Criteo Partner Pixel is loaded onto the website.

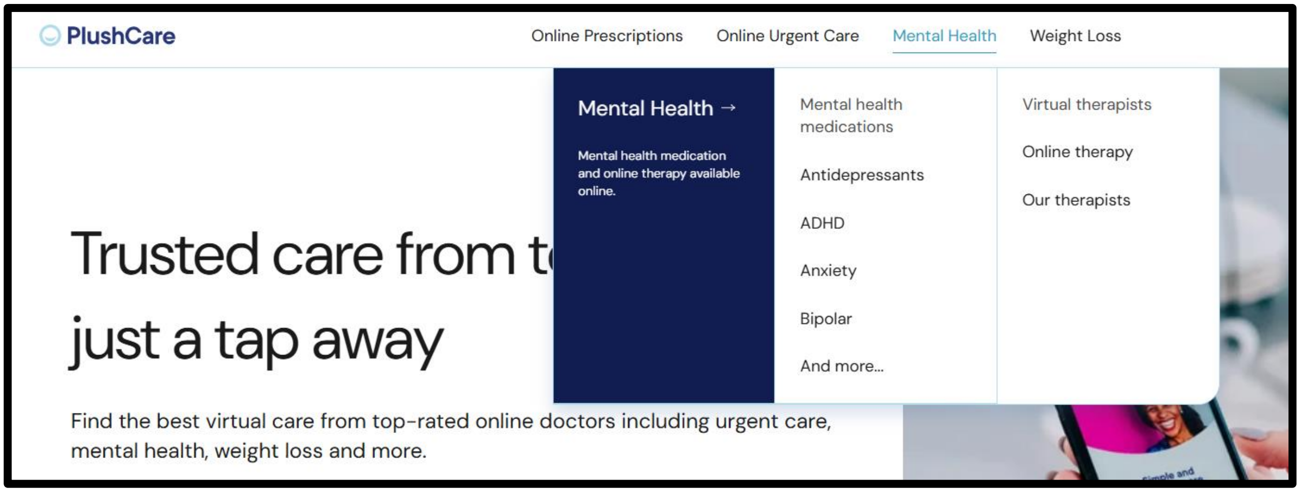
217. When a user selects the condition for which they are seeking treatment, that information is contained in a detailed descriptive URL as described above.



```
https://ib.adnxs.com/getuid?https%3A%2F%2Fdis.criteo.com%2Fdis%2Frtb%2Fappnexus%2F
cookiematch.aspx%3Fappnxsid=%24UID        GET ib.adnxs.com
/getuid?https%3A%2F%2Fdis.criteo.com%2Fdis%2Frtb%2Fappnexus%2Fcookiematch.aspx%3Fa
ppnxsid=%24UID
Fri Feb 07 09:48:24 EST 2025
```



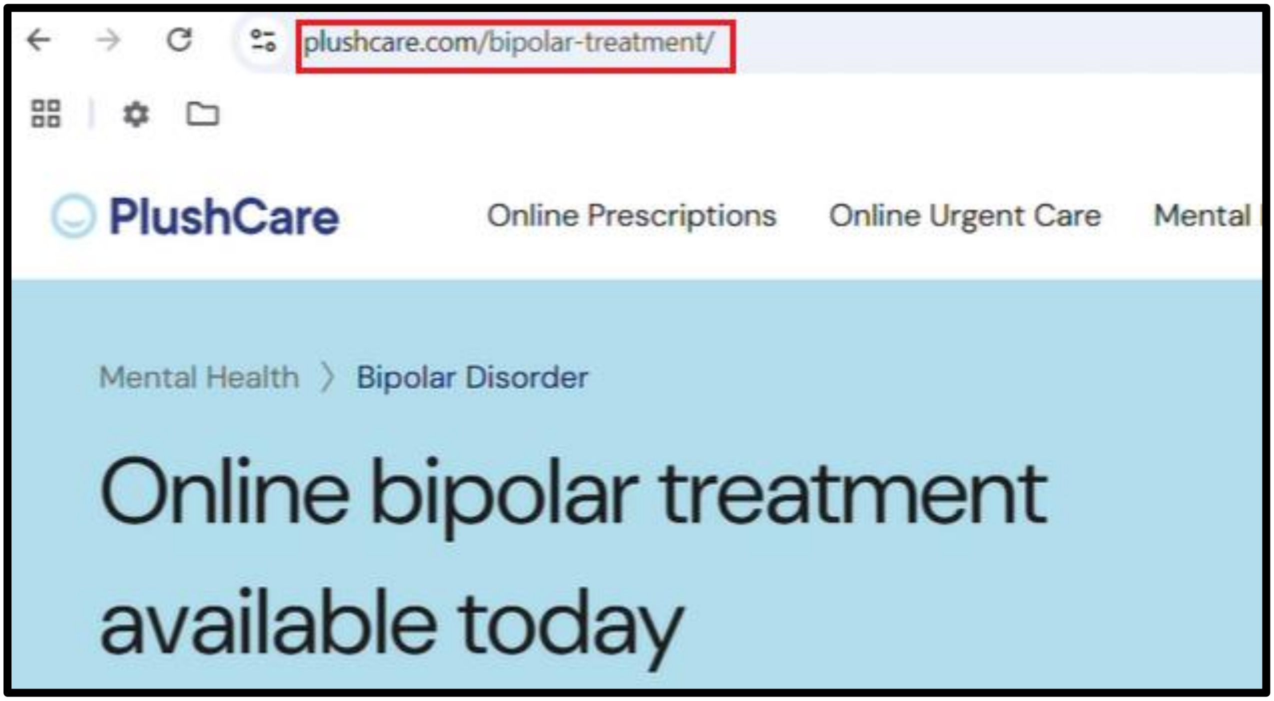
```
:authority: gum.criteo.com
:method: GET
:path: /syncframe?topUrl=plushcare.com&origin=onetag
:scheme: https
```



Mental health medication and online therapy available online.

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/
PlushCare
Online Prescriptions
Online Urgent Care
Mental
Mental Health 〉 Bipolar Disorder

Online bipolar treatment available today

218. 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.

219. The UID shared by Defendant allows Criteo and any other Partner Pixel to identify which individual is entering which information into the Plushcare website and, thus the Adnxs Pixel aids Criteo's wiretapping.

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

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

220. As a result of Microsoft technology being deployed on thousands or millions of websites, Defendant is collecting various forms of PII and web activity records of nearly every American and sells that data to target advsertising.

221. 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.

222. Defendant also combines the data from each and every website a person visits with other data collected by its partner advertisers. Further, through Microsoft's user ID syncing processes, Microsoft has access to not only its own information that it tracks from Internet users, but also the information that its partner advertisers track.[157] In this way, Microsoft amasses and aggregates Internet users' data and sells it back to its' partner advertisers. According to Microsoft, its clients can seamlessly integrate with major ad networks, exchanges, aggregators, and SSPs to buy data.[158] Microsoft notes that some of its key inventory supply partners are: Google Ad Manager, Microsoft Ad Exchange, Yahoo Ad Exchange, OpenX, Pubmatic, and The Rubicon Project, some of the largest players in the data-sharing space.[159]

[157] Microsoft, *supra* note 76.

[158] *About Microsoft Monetize*, Microsoft (May 10, 2024), https://learn.microsoft.com/en-us/xandr/monetize/about-monetize.

[159] *Exchanges and Aggregators*, Microsoft (Mar. 2, 2024), https://learn.microsoft.com/en-us/xandr/monetize/exchanges-and-aggregators.

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

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

224. The Microsoft identity resolution process is a key part of a complex ecosystem of pixels that deliver detailed user information to advertisers to increase the efficiency of those advertisements.

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

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

227. 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.

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

229. 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.

230. 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.

IV. PLAINTIFFS' EXPERIENCES

A. Plaintiff Stacy Penning

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

232. Unbeknownst to Plaintiff Penning, the Adnxs Pixel was loaded onto each page of the website.

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

234. The Adnxs Pixel collected information about Plaintiff Penning, including the webpages he visited, his IP address, and fingerprint information about his device and browser, among others.

235. Defendant shared Plaintiff Penning's IP address, Microsoft ID, previously collected information, and information about which pages of the Buzzfeed website he visited with every Partner Pixel to which it provided identity resolution through the Adnxs Pixel.

236. 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.

237. 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 and wiretapping his communications with websites.

238. Plaintiff Penning was unaware that Defendant was installing trackers on his browser, 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 Penning have discovered these facts.

239. 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.

240. 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.

B. Plaintiff SungGil Hong

241. In or about December 2024, Plaintiff SungGil Hong visited the AliExpress website while in California and viewed a bike rack for sale on the website.

242. Unbeknownst to Plaintiff Hong, the Criteo Pixel was loaded onto each page of the AliExpress website.

243. The Criteo Pixel, by receiving the detailed URL of each page of the website, intercepted Plaintiff Hong's confidential communications with the AliExpress website.

244. Unbeknownst to Plaintiff Hong, the Adnxs Pixel was loaded onto each page of the website.

245. These interceptions happened in real time as Plaintiff Hong searched for goods on the website.

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

247. When Plaintiff Hong visited the AliExpress website, The Adnxs Pixel installed multiple separate cookies onto Plaintiff Hong's browser.

248. The Adnxs Pixel collected information about Plaintiff Hong, including the webpages he visited, his IP address, and fingerprint information about his device and browser, among others.

249. Defendant shared Plaintiff Hong's IP address, Microsoft ID, previously collected information, and information about which pages of the AliExpress website he visited with every Partner Pixel to which it provided identity resolution through the Adnxs Pixel.

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

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

252. Plaintiff Hong 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 Hong have discovered these facts.

253. Plaintiff Hong 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.

254. Plaintiff Hong 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 Hong.

C. Plaintiff Laura Bonetti

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

256. Unbeknownst to Plaintiff Bonetti, the Adnxs Pixel was loaded onto each page of the website.

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

258. The Adnxs Pixel collected information about Plaintiff Bonetti, including the webpages she visited, her IP address, and fingerprint information about her device and browser, among others.

259. Defendant shared Plaintiff Bonetti's IP address, Microsoft ID, 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 Adnxs Pixel.

260. 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.

261. 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.

262. 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.

263. 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.

264. 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.

265. 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

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

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

268. The Bing Pixel, intercepted Plaintiff Hong's confidential communications with the Expedia website, including information about her travel.

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

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

271. 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.

272. 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.

273. 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.

274. 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.

275. 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.

276. Plaintiff Dantignac did not discover these violations until January 2025.

E. Plaintiff Jonathan Finestone

277. Multiple times in 2024, including in or about July 2024, Plaintiff Jonathan Finestone visited the Hyatt website and made a reservation.

278. Unbeknownst to Plaintiff Finestone, the Adnxs Pixel was loaded onto the Hyatt website.

279. When Plaintiff Finestone visited the Hyatt website, The Adnxs Pixel installed multiple separate cookies onto Plaintiff Finestone's browser.

280. As Plaintiff Finestone selected his hotel and dates of stay and made his purchase (i.e. in real time), the Adnxs Pixel intercepted that information.

281. The Adnxs Pixel then shared the information about Plaintiff Finestone's reservation with Partner Pixels loaded on the Hyatt website.

282. The Adnxs Pixel also collected information about Plaintiff Finestone, including the webpages he visited, his IP address, and fingerprint information about his device and browser, among others.

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

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

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

286. Plaintiff Finestone was unaware that Defendant was installing trackers on his browser, 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 Finestone have discovered these facts.

287. Plaintiff Finestone did not provide her 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.

288. Plaintiff Finestone 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 Finestone.

F. Plaintiff Robert Mason

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

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

291. 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.

292. Unbeknownst to Plaintiff Mason, the Adnxs Pixel was loaded onto each page of the website.

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

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

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

296. The Adnxs Pixel collected information about Plaintiff Mason, including the webpages he visited, his IP address, and fingerprint information about his device and browser, among others.

297. Defendant shared Plaintiff Mason's IP address, Microsoft ID, 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 Adnxs Pixel.

298. 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.

299. 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.

300. Plaintiff Mason 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 Mason have discovered these facts.

301. 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.

302. 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 ALLEGATIONS

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

> All persons in the United States whose personal information, communications, or private information, or data derived from their personal information, communications, or private information, was used to create a profile and/or made available for sale or use through Defendant's Microsoft Invest, Microsoft Monetize, or Microsoft Curate Products, distributed or sold in the process of delivering advertising on websites, mobile applications, or ither digital media, or otherwise.

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

> All California citizens in the United States whose personal information, communications, or private information, or data derived from their personal information, communications, or private information, was used to create a profile and/or made available for

> sale or use through Defendant's Microsoft Invest, Microsoft Monetize, or Microsoft Curate Products, distributed or sold in the process of delivering advertising on websites, mobile applications, or ither digital media, or otherwise.

305. 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.

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

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

308. **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.

309. **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.

310. **Commonality/Predominance**. Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members because

Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

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

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

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

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

311. **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

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

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

314. Plaintiffs bring this claim pursuant to California law.

315. 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).

316. 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.

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

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

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

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

(a) Defendant engages in widespread data collection and interception of Plaintiffs' and Class Members' internet and app activity, including their communications with websites and apps, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.

(b) Defendant combines the information collected on websites and apps with offline information also gathered on individuals to create the profiles used in the Microsoft products described herein.

(c) Defendant creates comprehensive profiles based on this online and offline data, which violates Plaintiffs' Class Members' common law right to privacy and the control of their personal information.

(d) Defendant sells or discloses these profiles, which contain the data improperly collected about Plaintiffs and Class Members, to an unknown number of advertisers for use in the real-time-bidding process, which likewise violates

Plaintiffs' Class Members' common law right to privacy and
the control of their personal information.

321. 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.

322. 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.

323. 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)

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

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

326. 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.

327. 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.").

328. 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).

329. 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.

330. 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.

331. Defendant's various pixels and SDKs, including the Adnxs and Bing Pixels are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

332. 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).

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

334. 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.

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

Members' confidential communications.

336. 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.

337. The wiretapping of Plaintiffs and California Subclass Members occurred in California, where Plaintiffs and California Subclass Members accessed the websites, where Defendant's pixels were loaded on Plaintiffs' and California Subclass Members' browsers, and where Defendant routed Plaintiffs' and California Subclass Members' electronic communications to Defendant's servers.

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

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

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

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

341. 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."

342. 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).

343. 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).

344. 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.

345. 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.

346. Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology has advanced, however, courts have expanded the application of these surveillance devices. This, combined with the California Supreme Court's mandate to read provisions of the CIPA broadly to protect privacy rights, has led courts to apply CIPA § 638.50 to internet tracking technologies similar to Defendant's technologies at issue here. *See, e.g., Shah v. Fandom, Inc.*, --- F. Supp. 3d ---, 2024 WL 4539577, at *21 (N.D. Cal. Oct. 21, 2024) (finding trackers were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Lesh v. Cable News Network, Inc.*, --- F. Supp. 3d ---, 2025 WL 563358, at *3-5 (S.D.N.Y. Feb. 20, 2025) (same); *Moody v. C2 Educ. Sys. Inc.*, 742 F. Supp. 3d 1072, 1076 (C.D. Cal. 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and 638.51."); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (referencing CIPA's "expansive language" when finding software provided by data broker was a "pen register").

347. The Microsoft Pixels Microsoft 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.

348. At all relevant times, Defendant installed the Microsoft Pixels—which are pen registers—on Plaintiffs' and California Subclass Members' browsers, which enabled Defendant to collect Plaintiffs' and California Subclass Members' IP addresses, geolocation, device information, and other persistent identifiers from the websites they visited. Defendant then used the pixels 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.

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

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

351. 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

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

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

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

355. 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.

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

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

358. 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.

359. 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.

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

361. 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.

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

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

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

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

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

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

367. 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.

368. 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).

369. 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).

370. 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).

371. 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).

372. 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).

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

(a) The Adnxs Pixel;

(b) The Bing Pixel;

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

(d) Each Partner Pixel.

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

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

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

377. 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).

378. 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.

379. 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).

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

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

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

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

PRAYER FOR RELIEF

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: April 1, 2025

Respectfully submitted,

By: */s/ Wright A. Noel*
Wright A. Noel

CARSON NOEL PLLC
Wright A. Noel (WSBA #25264)
20 Sixth Avenue NE
Issaquah, WA 98027
Telephone: (425) 395-7786
Email: wright@carsonnoel.com

BURSOR & FISHER, P.A.
Philip L. Fraietta (*Pro Hac Vice* forthcoming)
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) 837-7408
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com
mroberts@bursor.com
vzhou@bursor.com

BURSOR & FISHER, P.A.
Joshua R. Wilner (*Pro Hac Vice* forthcoming)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: jwilner@bursor.com

Attorneys for Plaintiffs

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

STACY PENNING, ET AL., individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff ____________
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Carson & Noel PLLC, 20 Sixth Avenue NE, Issaquah,
WA 98027; (425) 395-7786

DEFENDANTS

MICROSOFT CORORATION

County of Residence of First Listed Defendant KING
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

☐ 1 U.S. Government Plaintiff
☐ 3 Federal Question *(U.S. Government Not a Party)*
☐ 2 U.S. Government Defendant
☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT

☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

REAL PROPERTY

☐ 210 Land Condemnation
☐ 220 Foreclosure
☐ 230 Rent Lease & Ejectment
☐ 240 Torts to Land
☐ 245 Tort Product Liability
☐ 290 All Other Real Property

TORTS

PERSONAL INJURY

☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Federal Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
☐ 360 Other Personal Injury
☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY

☐ 365 Personal Injury - Product Liability
☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY

☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

CIVIL RIGHTS

☐ 440 Other Civil Rights
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/ Accommodations
☐ 445 Amer. w/Disabilities - Employment
☐ 446 Amer. w/Disabilities - Other
☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:

☐ 463 Alien Detainee
☐ 510 Motions to Vacate Sentence
☐ 530 General
☐ 535 Death Penalty

Other:

☐ 540 Mandamus & Other
☐ 550 Civil Rights
☐ 555 Prison Condition
☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY

☐ 625 Drug Related Seizure of Property 21 USC 881
☐ 690 Other

LABOR

☐ 710 Fair Labor Standards Act
☐ 720 Labor/Management Relations
☐ 740 Railway Labor Act
☐ 751 Family and Medical Leave Act
☐ 790 Other Labor Litigation
☐ 791 Employee Retirement Income Security Act

IMMIGRATION

☐ 462 Naturalization Application
☐ 465 Other Immigration Actions

BANKRUPTCY

☐ 422 Appeal 28 USC 158
☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS

☐ 820 Copyrights
☐ 830 Patent
☐ 835 Patent - Abbreviated New Drug Application
☐ 840 Trademark
☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY

☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))

FEDERAL TAX SUITS

☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES

☐ 375 False Claims Act
☐ 376 Qui Tam (31 USC 3729(a))
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce
☐ 460 Deportation
☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 485 Telephone Consumer Protection Act
☐ 490 Cable/Sat TV
☐ 850 Securities/Commodities/ Exchange
☒ 890 Other Statutory Actions
☐ 891 Agricultural Acts
☐ 893 Environmental Matters
☐ 895 Freedom of Information Act
☐ 896 Arbitration
☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding
☐ 2 Removed from State Court
☐ 3 Remanded from Appellate Court
☐ 4 Reinstated or Reopened
☐ 5 Transferred from Another District *(specify)*
☐ 6 Multidistrict Litigation - Transfer
☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)(A)

Brief description of cause:
Intrusion Upon Seclusion

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ $5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE ____________ DOCKET NUMBER ____________

DATE
April 1, 2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Wright A. Noel

FOR OFFICE USE ONLY

RECEIPT # ________ AMOUNT ________ APPLYING IFP ________ JUDGE ________ MAG. JUDGE ________

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT

for the

Western District of Washington

STACY PENNING, SUNGGIL HONG, LAURA BONETTI, JONATHAN FINESTONE, TANISHA DANTIGNAC AND ROBERT MASON, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

MICROSOFT CORPORATION,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

Microsoft Corporation
Corporation Service Company
300 Deschutes Way SW, Suite 208
MC-CSC1
Tumwater, WA 98501

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Wright A. Noel
Carson & Noel PLLC
20 Sixth Avenue NE
Issaquah, WA 98027

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: ____________________

____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* ______________________________
was received by me on *(date)* ______________ .

❐ I personally served the summons on the individual at *(place)* ______________________
______________________________ on *(date)* ______________ ; or

❐ I left the summons at the individual's residence or usual place of abode with *(name)* ______________
______________________________ , a person of suitable age and discretion who resides there,
on *(date)* ______________ , and mailed a copy to the individual's last known address; or

❐ I served the summons on *(name of individual)* ______________________________ , who is
designated by law to accept service of process on behalf of *(name of organization)* ______________
______________________________ on *(date)* ______________ ; or

❐ I returned the summons unexecuted because ______________________________ ; or

❐ Other *(specify)*:

My fees are $ __________ for travel and $ __________ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: ______________

____
Server's signature

____
Printed name and title

____
Server's address

Additional information regarding attempted service, etc: