James M. Wagstaffe, Esq.
ADAMSKI MOROSKI MADDEN CUMBERLAND & GREEN LLP
P.O. Box 3835
San Luis Obispo, CA 93403-3835
Tel: 805-543-0990
Fax: 805-543-0980

Christian Levis (*pro hac vice* forthcoming)
clevis@lowey.com
Amanda Fiorilla (*pro hac vice* forthcoming)
afiorilla@lowey.com
Rachel Kesten (*pro hac vice* forthcoming)
rkesten@lowey.com
Yuanchen Lu (*pro hac vice* forthcoming)
ylu@lowey.com
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035

Attorneys for Plaintiff and The Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JENNIFER TURNER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

THE TRADE DESK, INC.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jennifer Turner, individually and on behalf of all other similar situated individuals, asserts the following against Defendant The Trade Desk, Inc. ("the Trade Desk") based upon personal knowledge, information and belief (where applicable), and the investigation of counsel. The Court has jurisdiction over these claims as stated in Paragraphs 34 through 36.

SUMMARY OF ALLEGATIONS

1. Individuals using internet-connected devices have a baseline expectation of privacy, in which they do not expect any company to engage in wide-spread surveillance of all their online activity.

2. Consistent with this expectation, companies have moved away from traditional means of user-based online tracking in recognition that they are ***privacy invasive***. This includes features like Apple, Inc.'s "Do Not Track" setting, which prevents the collection of advertising IDs from mobile device users, as well as the planned deprecation of third-party cookies, which are used to track users across multiple websites.

3. The Trade Desk saw this trend away from traditional ad-targeting tools as an opportunity to build a new form of online tracking that circumvented existing privacy controls. It calls this "Unified ID" which it first launched in 2018. It released a new version, called Unified ID 2.0 ("UID2"), in 2020.

4. Through these identity "solutions"—and complimentary products (e.g., its Universal Pixel)—the Trade Desk has been secretly harvesting and monetizing directly identifiable user data from millions of U.S. residents without their knowledge.

5. The first version of Unified ID ("UID1") was created by the Trade Desk as a unique identifier that serves as a replacement for traditional third-party cookies. It remains consistent on all websites that have adopted this ID, which allows a user to be tracked across the internet. Thus, if a user visits Walmart, then Etsy, and Noom, the same UID1 is assigned to that user because they all recognize UID1. This can be observed in network traffic as a "TDID" cookie.

6. The UID2 is even more privacy-invasive. The UID2 framework intercepts directly identifiable information (i.e., users' email addresses and/or phone numbers) whenever they log-in, create an account, or take other actions on the webpage that recognizes this identifier. It then returns a UID2 (either in raw or tokenized form) to the website operator directly keyed-off this personally identifying information.

7. The Trade Desk designed UID2 so that (like UID1) it is consistent (and persistent) across every ***other*** website, mobile application, connected-TV, and other platforms, that uses UID2. Thus, whenever the Trade Desk receives an email address or phone number from a different website, app, or other service, they assign the same UID2 that is already associated with that unique email address or phone number.

8. Because UID2 is not a cookie, it circumvents traditional privacy-preserving mechanisms. For instance, while traditional cookies typically expire after a limited period of time and can be reset; individuals' email addresses and phone numbers are permanent identifiers. By creating an identifier tied to personally identifiable information that does not change, the Trade Desk has created a permanent identity tracking mechanism.

9. UID1 and UID2 were wildly successful and can be found across websites, mobile applications, TV products, and streaming services. Because these identifiers are both unique and persistent, the Trade Desk created a way to track users ***everywhere***.

10. In addition to providing an identity solution, the Trade Desk also offers unique ways for companies to monetize the value of UID1 and UID2, as well as users' data associated with those identifiers.

11. This includes offering targeted advertising tools. For instance, companies can embed the Trade Desk's Universal Pixel on their website to directly intercept users' online interactions and private communications, track their activity, and create actionable insights. The Trade Desk then processes this information—associates it with UID1 and/or UID2—and offers companies the ability to create custom audiences (group-based targeting) and lookalike audiences (i.e., finding similar users based off existing users' data), among other advertising capabilities.

12. Another, separate way the Trade Desk harvests users' data and leverages the power of its UID2 is through real-time bidding—i.e., the auction-like process that determines the ads users see on websites or other web properties they visit.

13. The Trade Desk is one of the fastest growing entities operating as a demand-side platform ("DSP") in the real-time bidding process. A DSP acts as a middleman between a publisher (the person offering ad space) and the advertiser (the person showing the ad).

14. The Trade Desk's DSP allows advertisers to bid on "impressions" (i.e., ad space) in real time based on personally identifiable user data associated with that individual's UID1/ UID2. This includes data the Trade Desk has collected from both the ***advertiser and the publisher*** to facilitate the ad-purchasing process.

15. With troves of data from both the advertiser and publisher associated with the same unique identifier, the Trade Desk has positioned itself to be a dominant force in targeted advertising because it knows exactly who is the best fit to see any given advertisement at any given time, unlike other competitors.

16. The Trade Desk directly profits from facilitating this hyper-specific form of ad targeting. The Trade Desk reports that a "record" $12 billion has been spent on the Trade Desk platform and that it has made over $2.4 billion in revenue.

17. Plaintiff and Class Members had no knowledge that the Trade Desk was using unique identifiers to track them across the web, mobile applications, and other internet-connected devices, or that it was using this data to facilitate highly specific targeted advertising. The Trade Desk itself offers no consumer facing policies or disclosure, nor does it prompt users viewing the websites or other web properties that use its identifiers of its presence, data collecting, or processes.

18. The Trade Desk's interception of the contents of their communications with third parties through its tracking technology violates Cal. Penal Code § 631, and its installation of a tracking device on each of the websites they use across the internet violates Cal. Penal Code § 638.51(a), as well as other laws.

PARTIES

A. Plaintiff

19. Plaintiff Jennifer Turner is a resident of Tulare County, California.

20. Plaintiff Turner used several online services, including Etsy and Noom, that implemented the Trade Desk's identifiers and tracking software.

21. For each of these services, Plaintiff created an account and logged-in using her email address.

22. Unbeknownst to Plaintiff Turner, the Trade Desk intercepted her personal email address from online services she used, processed this information, and assigned her a UID2. The Trade Desk returned the UID2 to these services in either "raw" or tokenized form.

23. Many of these websites, including Etsy and Noom, also use the Trade Desk's Universal Pixel. Through this technology, the Trade Desk intercepted the UID2 it assigned to Plaintiff Turner, as well as the contents of her communications with Etsy and Noom, such as the specific pages she viewed or the content of her searches. The Trade Desk processed this data and stored it on its own servers to target Plaintiff Turner with its customer's ads.

24. The Trade Desk used the UID2 (and UID1) to continue to track Plaintiff Turner across the web, mobile devices, connected TVs, and other platforms.

25. When Plaintiff Turner visited websites or used services operated by participating publishers, the Trade Desk used Plaintiff Turner's UID2 to recognize her as the intended recipient of a targeted advertisement.

26. Acting as a DSP, The Trade Desk used Plaintiff Turner's UID2, along with data reflecting her online communications, to facilitate real-time bidding for ad space that would ultimately be served to her. Thus, the Trade Desk directly profited as a DSP through the use of Plaintiff Turner's identifiable data.

27. Plaintiff Turner did not consent to the Trade Desk intercepting her personally identifiable information, assigning and using unique identifiers to track her across internet-enabled services and devices, or intercepting and using the contents of her private communications for-profit.

B. Defendant

28. The Trade Desk is a Delaware corporation with its principal place of business located in Ventura, California.

29. The Trade Desk knowingly and intentionally developed persistent, unique identifiers to track Plaintiff and Class Members across internet-connected services.

30. The Trade Desk knew that its identifiers, and especially UID2, circumvented existing privacy protections (such as "Do Not Track" and widespread adoption of third-party cookie blocking by

major browsers like Safari and Firefox) because it developed this identifier specifically as an alternative to such privacy-preserving mechanisms.

31. The Trade Desk offered these services to websites, mobile applications, television providers, and other services so that it would have a unique way of tracking Plaintiff and Class Members across devices and platforms.

32. The Trade Desk knowingly and intentionally used its identifiers, and data associated with it, to facilitate targeted advertisements for profit.

33. The Trade Desk marketed its technology as offering privacy-preserving ad capabilities, despite understanding it created persistent identifiers, including UID2, that is directly tied to permanent, directly identifiable information, like email and phone number.

JURISDICTION AND VENUE

34. Jurisdiction is proper under 28 U.S.C § 1332(d) because: (1) the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, (2) there are more than 100 putative members of the Class, and (3) a significant portion of Class Members are citizens of a state different from the Trade Desk.

35. This Court has personal jurisdiction over the Trade Desk because its principal place of business is in California. Additionally, this Court has personal jurisdiction over the Trade Desk because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in California, including the Trade Desk's interception and use of Plaintiff's personally identifiable information.

36. Venue is proper under 28 U.S.C. §1391(b), (c), and (d) because a substantial portion of the conduct described in this Class Action Complaint was carried out in this District. The Trade Desk maintains substantial business operations in this District, including, upon information and belief, activities implementing the Trade Desk's identity resolution products and Unified ID 2.0, and demand-side platform, managing data partnerships, and facilitating the sale of data through real-time bidding auctions.

37. Pursuant to Civil L.R. 3-2(c), the assignment to the division is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in this District. Trade Desk's conduct,

as described herein, is directed at Internet users and people throughout the United States, including in San Francisco County California, where the Trade Desk maintains offices and business operations.

BACKGROUND OF USER TRACKING

38. Over a decade ago, Apple, Inc. announced that it would no longer allow app developers to intercept "UDIDs" which are unique, device-specific identifiers. These persistent identifiers were deprecated because they are seen as privacy intrusive—they cannot be reset and were used to facilitate device-specific targeted advertising.

39. Starting in 2020, Apple, Inc. and Google, LLC rocked the digital advertising world once again by announcing the eventual depreciation of advertising identifiers (IDFA and ADID) and third-party cookies in favor of more privacy-preserving mechanisms. Advertising identifiers were seen as a replacement for UDIDs because they could be reset by the user, as can third-party cookies. However, this did not change that they are ultimately privacy-invasive, as they allow ad targeting at the user level.

40. This created serious concerns within the multi-billion dollar digital advertising industry. Digital advertisers relied on these device identifiers and cookies to uniquely identify individuals who use their products and services—and other entities' products and services—to curate and serve targeted advertisements to individuals, based on profiles of information reflecting web and app activity indexed to unique identifiers present in third-party cookies.

41. For instance, a mobile app developer would use identifiers like the IDFA and ADID created by iOS and Android phones, to track user activity across their mobile application, understand what actions users took and their preferences, interests, and other information. The company would then send that information to an advertising company, such as Google, to serve targeted advertisements to that customer using this unique identifier.

42. While companies scrambled to find solutions to the eventual depreciation of unique device identifiers and third-party cookies, many options were not nearly as lucrative. For instance, many companies began tracking "sessions" (i.e., one interaction with the webpage) and then sought to use cross-device tracking alternatives to match each of these unique sessions to the same user. However, this alternative is not nearly as powerful as directly tracking an individual at the ***user***-level rather than ***session***-level.

THE TRADE DESK'S UNIQUE IDENTIFIERS

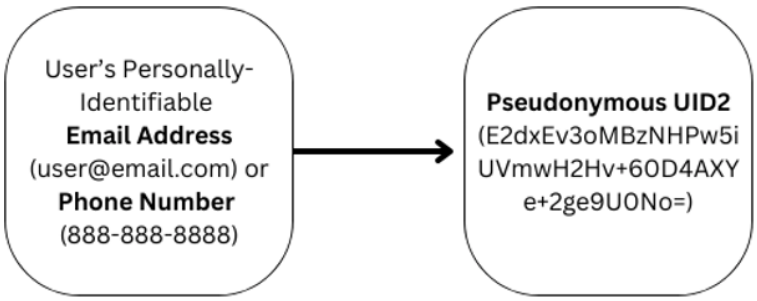
43. Enter the Trade Desk. The Trade Desk capitalized on the move away from device identifiers and third-party cookies by Apple and Google by creating a persistent unique, cross-platform identifier ***of its own***.

44. The first identity solution was called Unified ID 1.0 (UID1). This is reflected in network traffic as "TDID." This identifier was developed as a replacement to traditional third-party cookies. The UID1 is consistent across websites. Thus, if a user logs in to Marriot, then Etsy, and then another website that uses UID1, the Trade Desk—and its partners—understands this is the same user and can link all their online activity to the same identifier.[1]

45. The Trade Desk went on to develop Unified ID 2.0 ("UID2"). While billed as an "open-source identity solution" that is "privacy-conscious", it is just the opposite.

46. UID2 works by intercepting personally identifiable data (which the Trade Desk calls "directly identifying information" ("DII")), such as email addresses and phone numbers, and assigns a pseudonymized identifier in its place.

FIGURE 1



47. The Trade Desk refers to this as the "raw" UID2.

48. Because this DII is mapped to a unique UID2, individuals remain personally identifiable by all entities that use the Trade Desk platform. For instance, each time a user provides their email address or phone number to an online service that uses UID2, this information is intercepted and hashed by the UID2 Operators.

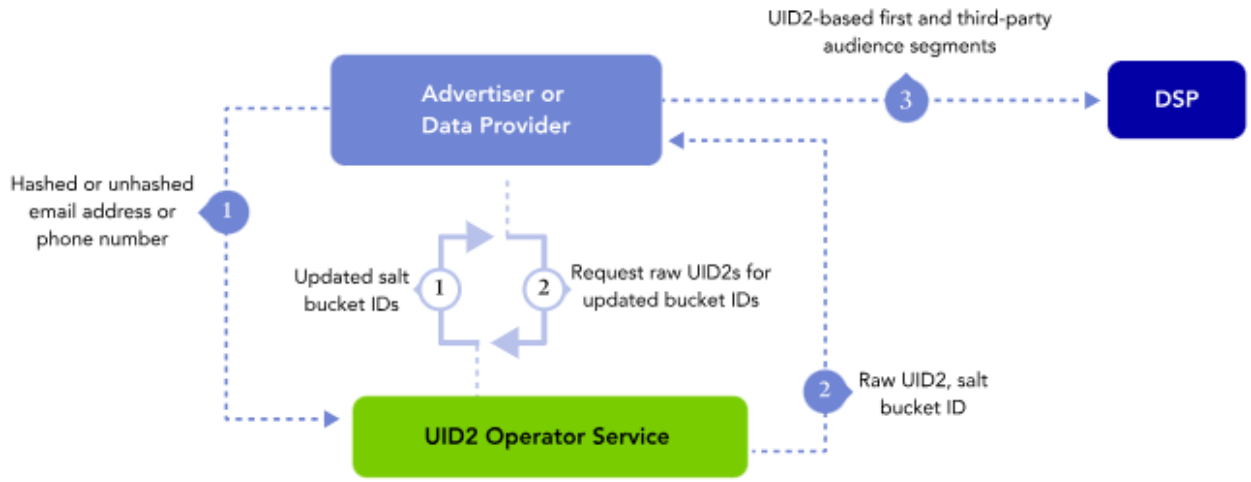
[1] Companies that use TDID include Noom, OldNavy, Marriot, Esty, Buzzfeed, Walmart, and Variety. Thus, if a consumer visited all of these websites, they are tracked consistently and identified by the same TDID.

49. UID2 "Operators" run, in essence, a directory that allows entities to look up a specific individuals' identity profile based on submitted DII. The UID2 Operator processes DII submitted by website or app developers and either assigns a new UID2 to that user or returns the existing value mapped to the DII submitted. Because the UID2 remains the same for each user based on their DII, it can then be used to track their activity across the website or service.

50. There are two types of Operators who perform this interception: Public Operators and Private Operators. The Trade Desk itself operates as the Public Operator for UID2. Thus, the Trade Desk is the primary entity that intercepts users' email addresses and phone numbers and the entity who sends back to the website the UID2 identifier. By default, the UID2 is stored in the user's local storage, rather than as a typical cookie.

51. Trade Desk recommends that online services use a "Public Operator" (i.e., itself) over Private Operators. Figure 2 describes how this process works:

FIGURE 2[2]



52. Importantly, UID2 is a form of pseudonymized—***not*** anonymized—data. This mean it remains identifiable because it is tied to actual underlying DII. Thus, while UID2 does not contain the users' actual email address or phone number, it serves as the functional equivalent of those values based on its direct mapping to them.

[2] https://unifiedid.com/docs/overviews/overview-data-providers

53. The Trade Desk's use of hashing in this process does not protect users' emails and phone numbers, or render the data anonymous. Indeed, this methodology has been ***repeatedly criticized***, including by the Federal Trade Commission.

54. The Federal Trade Commission has confirmed that "hashing" email addresses and phone numbers that always return the same identifying number (like here) is both an "old" and "flawed" methodology because the hashes are not "anonymous" and "can still be used to identify users, and their misuse can lead to harm." It cautions: "[c]ompanies should not act or claim as if hashing personal information renders it anonymized."

55. Based on how UID2 is configured, every time a user enters the same email address or phone number on ***another*** website or platform, the same UID2 is used.

56. The Trade Desk admits this: "the process of generating a raw UID2 from DII is the same, and results in the same value, no matter who sent the request."

57. Therefore, the UID2 tracks the user across all websites or online services that use UID2, so long as the user logs in or creates an account using the same identifying email or phone number.

58. Especially problematic, UID2 is a ***stronger*** identifier than those that previously existed. For instance, first-party cookies are limited in that they only track a user on one specific website. UID2 goes ***further*** by tracking users across ***all*** websites and apps using this identifier. This makes it possible to create an identity profile that serves advertisers' needs, by aggregating data across all apps and websites a person uses, at the expense of individual's right to privacy.

59. Moreover, while cookies expire or can be reset, UID2 is directly tied to email addresses and phone numbers, which are permanent identifiers. Thus, they cannot be reset or time-out in the same way as cookies.

60. The UID2 has been widely adopted and used by the Trade Desk to provide targeted advertising, including through lookalike audiences, conversion tracking, and real-time bidding, described further below.

THE TRADE DESK'S TARGETTING SERVICES

61. The Trade Desk created UID2 as a catalyst to position itself as a go-to partner for advanced advertising targeting. To achieve this, the Trade Desk created ***complimentary products*** that use UID2 to track and "activate" users' data directly with the Trade Desk.

62. One of the products the Trade Desk offers is the Trade Desk Universal Pixel. Using this pixel, the Trade Desk intercepts the UID2 and online users' private communications directly from webpages and redirects it to its own servers so it can be used for advertisements, including the creation of custom audiences, lookalike audiences, and campaign optimization.

FIGURE 3[3]

REPRESENTATIVE EXAMPLES OF UID2 & THE UNIVERSAL PIXEL

63. The Trade Desk openly advertises the capabilities of using all its products together. For instance, in one case study, the Trade Desk boasts that a "luxury hotel" adopted UID2. It then used the Trade Desk's Universal Pixel—like the websites used by Plaintiff—to understand and target users who took certain actions, such as adding products to their cart. It claims the results were "outstanding" and resulted in "well over 200 bookings."

64. Several other entities have adopted both UID2 and the Trade Desk's Universal Pixel given their complementary nature.

65. For instance, when a user visits Marriott's website, this triggers both a UID2 token and the Trade Desk Universal Pixel. This can be observed in network traffic.

[3] https://unifiedid.com/docs/sharing/sharing-use-cases

66. First, the Trade Desk's initial loader executes, loading the UID2 framework, and preparing to perform identity matching, as indicated by up_loader.1.1.0.js. This establishes the Trade Desk as the Operator for Marriott.

67. The next the Trade Desk Universal Pixel code runs through the execution of universal_pixel.1.1.0.js. During this process, the Trade Desk's code intercepts and processes DII (e.g., email or phone number), and then checks for existing UID2 and the TDID (the Trade Desk's UID1). This information is returned to Marriott in either tokenized or raw form. If an UID2 does not exist, The Trade Desk prepares and returns a new one.

68. The Trade Desk Universal Pixel code then initiates a connection to a Trade Desk domain: insight/adsrvr.org/track/up. This is where data captured by the Pixel is rerouted back to Trade Desk, including UID1 (observed as TDID) and UID2. The Trade Desk not only receives these unique identifiers, but also information about the user's interaction on Marriott. For instance, if the user searched for hotels in Clearwater, Florida, the Pixel relays that information through a full-string URL to the Trade Desk.[4] The Trade Desk also receives—as a required field—the "adv" parameter, reflecting the ID for the specific website visited by the user.

69. As another example, Esty—which Plaintiff used—also runs the Trade Desk UID2 framework and functions in the same way. When users visit or log-in to Etsy, the Trade Desk's code runs in the background. It detects and intercepts directly identifiable information (e.g., email addresses), and assigns or generates the existing UID2. The Universal Pixel transmits the UID2 and other information about the user back to the Trade Desk. For instance, if a user searches on Etsy for a product, the Trade Desk receives the exact search the user input, alongside the UID2 token and other information. The Trade Desk also receives—as a required field—the "adv" parameter, reflecting the ID for the specific website visited by the user.

70. The same is true for WeightWatchers. When a user visits or logs-in to WeightWatchers, the Trade Desk's code is waiting in the background to intercept directly identifiable information to assign

[4] Especially problematic, it is clear this data does not stay with the Trade Desk itself. This is clear from the TDCPM cookie, which is (yet again) offered by the Trade Desk. This cookie is used to share the UID2 token, as well as additional information like the user's activity on the website, with additional third parties. The TDCPM cookie on the Marriott website shows companies like LiveRamp and AppNexus also receive this data.

or generate a UID2. The WeightWatchers website also incorporates the Universal Pixel, through which the Trade Desk intercepts UID2 and/or UID1 (observed as TDID), as well as the content of users' communications with WeightWatchers. Thus, if a user visits WeightWatcher's weight-loss medication page, the Trade Desk intercepts the UID2 and/or UID1, alongside full the URL string and can discern that the user is interested in or takes weight loss medication. The Trade Desk also receives—as a required field—the "adv" parameter, reflecting the ID for the specific website visited by the user.

71. As a final example, the Trade Desk's UID2 framework and Universal Pixel is also present on the Noom website, another web property Plaintiff engaged with. Like above, the Trade Desk intercepts DII to assign and generate a UID2. If a Noom user opts to complete a Noom survey for weight-loss medication, the Trade Desk's Universal Pixel intercepts this information, including UID2 and/or UID1, as well as data reflecting that the user is completing a "clinical" survey. The Trade Desk also receives—as a required field—the "adv" parameter, reflecting the ID for the specific website visited by the user.

72. The Trade Desk also permits online services to send data directly to the Trade Desk, which avoids detection, as such data transfers cannot be observed by reviewing network traffic. This compounds the egregiousness of the Trade Desk's privacy violation, as so much of its conduct already occurs in secret.

THE USE OF UID2 FOR REAL-TIME BIDDING

73. One of the other primary ways UID2 is used is during a process known as ***real-time bidding***, described briefly below.

74. When a user visits a website or other service, it may use "programmatic ads." In those instances, the website owner is known as an ad "Publisher."

75. Publishers share "authenticated" personally identifiable information, like email addresses, with UID2 Operators prior to creating what is known as a "bid request." The Operators (e.g., the Trade Desk) then return a UID2 Token that is sent alongside the ultimate bid request. If a Publisher opts to send an existing UID2 token (rather than DII directly), UID2 Operators decrypt this information to identify the individual.

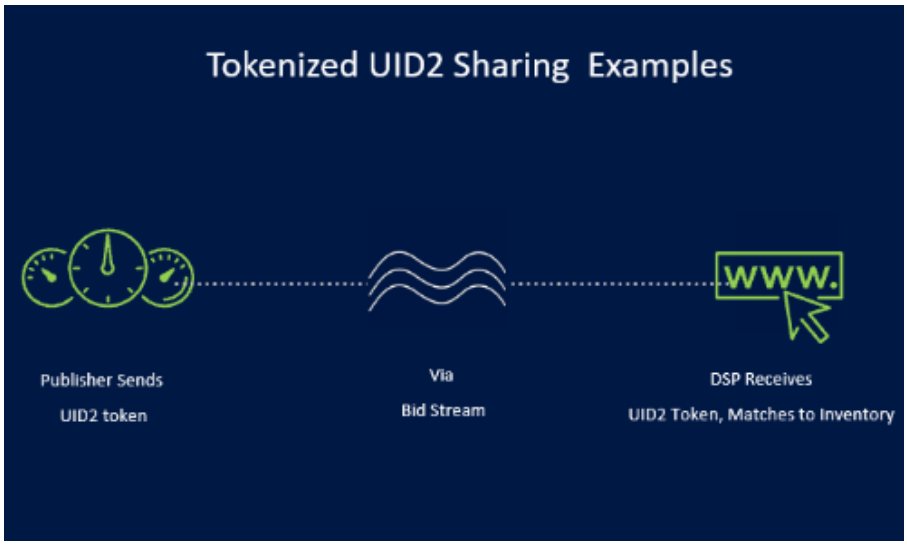
76. In addition to UID2, the bid request typically contains other information from the Publisher about the user who is going to see the eventual ad (e.g., additional user information such as

location, demographics, and behaviors), ad details (e.g., format, size, placement, URL), and auction information (such as Auction ID, time to respond, etc.).

77. The Publisher pushes the UID2 and bid request into what is known as the "bid stream."

78. The Trade Desk also sits on the other side of this transaction as a DSP. In this role, the Trade Desk receives the bid steam, alongside UID2, which it then ***decrypts*** at the time of the bid request to understand who will ultimately see the ad and match it to potential advertisers interested in that user.

FIGURE 3[5]



79. As a DSP, the Trade Desk ***also*** receives information from the potential advertiser. This includes information such their potential ad campaign, including their budget (i.e., the maximum and minimum amount they are willing to pay), what the ad will look like and contain, as well as targeting criteria and identity data, including UID2.

80. If the potential ad space matches who the advertiser seeks to target (which the Trade Desk knowns through its ever-present UID2), the Trade Desk submits a real-time bid to the ad exchange to win the ad space.

81. This all happens in an auction that lasts milliseconds. Advertisers compete with one another to show their ad in the ad space based on how valuable it is to them to show that particular ad to that particular user. The highest bidder wins.

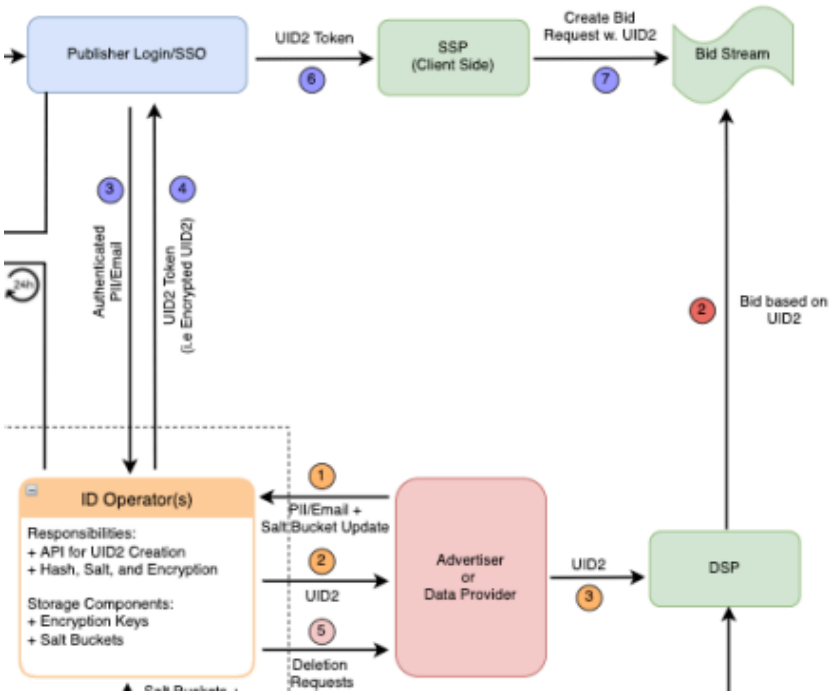
[5] https://unifiedid.com/docs/sharing/sharing-use-cases

82. Because the Trade Desk fully controls UID2 and receives this information from both the Publisher and the advertiser, it had unique insights that other DSPs lack and can better target individual users, including Plaintiff and Class Members.

83. The Trade Desk facilitates these types of hyper-specific targeted advertisements—all based on UID2—across platforms ranging from mobile phones and webspace, to inter-connected TVs.

84. Figure 4—which comes from the Trade Desk documentation—confirms how this process works. In this diagram, the Trade Desk acts as the "ID Operator" as well as the "DSP." As **Figure 4** shows, it receives DII directly from the publisher and advertiser and then uses UID2 to place the bid requests for profit.

FIGURE 4[6]



THE USE OF UID2 BY THIRD-PARTY DATA PROVIDERS

85. To make matters worse, it is not just website and app developers who are using UID2 to uniquely identify users. As reported by the Trade Desk's CEO, 75% of "third-party data ecosystem[s]"

[6] https://itega.org/wp-content/uploads/2021/01/Trade-Desk-UID2-Overview-Dec-2020.pdf

(i.e., data brokers) are also using UID2 as a way to identify users in their data sets. The ability to join commercially available data with UID2 makes all data collected by the Trade Desk identifiable.

86. Data brokers using UID2 to track and uniquely identify online users include Nielsen, Acxiom, Oracle, and Adobe, each of which maintains their own identity platform for linking data back to specific individuals to facilitate targeted advertising. The existence of these additional profiles only further confirms the identifiability of sensitive information collected by the Trade Desk.

87. Many data brokers provide this data directly to the Trade Desk, increasing its visibility into online users and its ability to target them with ads.

PLAINITFF AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION OF PRIVACY

88. The internet is not the Wild West. Internet users do not expect to be tracked across every single one of their internet-connected devices, including their web browser, apps, TVs, and more.

89. Indeed, the advent of privacy-preserving mechanisms like Apple's "Do Not Track" feature, which prevents companies from collecting IDFA/ADID from individuals who opt-out, have confirmed this expectation.

90. One study by Flurry Analytics in 2021 shows that 88% of iOS users worldwide have availed themselves of this feature, indicating an intent to prevent apps from tracking them on their mobile devices.

91. Users do not know—and did not expect—that the Trade Desk would circumvent these protections by creating a new identifier that is even ***better*** than IDFA/ADID at tracking them across services. Several privacy experts have warned that UID2 is especially problematic—going so far as to classify it as a "regression in privacy"—precisely because it subverts these privacy-preserving mechanisms (i.e., "Do Not Track" and private browsing mode).

92. The Trade Desk itself does not provide any information for Plaintiff and Class Members to understand which websites or online services use their UID2, such that they have no way of uncovering which services do or do not contain the Trade Desk's tracking technology. There is also no way for Plaintiff or Class Members to opt out of UID2 or to avoid the Trade Desk capturing, storing, and tracking their use of apps and websites, or its sharing of that data with third parties.

93. Plaintiff and Class Members reasonably expect that their online activity would not be tracked by an unknown company, let alone that it would be used to target them across online services for profit.

94. The Trade Desk did not have consent to perform this type of omni-present cross-device tracking using Plaintiff and Class Members' email addresses and phone numbers.

THE TRADE DESK UID2 VIOLATES ESTABLISHED DATA PRIVACY REGIMES

95. The Trade Desk markets itself as a company built with data-privacy protections in mind, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

96. The GDPR and CCPA both mirror Fair Information Practice Principles (FIPPs). Two of the core tenants of FIPPs are (1) clear user consent; and (2) data minimization.

97. The Trade Desk does neither of these things. Despite creating a cross-device persistent user identifier, the Trade Desk makes zero effort to ensure Plaintiff and Class Members are even ***aware*** of where this technology is used. This is clear from its own Privacy Policy, which makes no attempt to identify the entities using its services.

98. Separately, the creation of an ever-present persistent identifier is directly at odds with the idea of data minimization, which requires that data should be stored and used only for the period of time in which that data is necessary. Indeed, the fact that device and user-specific identifiers are persistent (and not deleted) is exactly why even device identifiers like IDFA are being phased out by companies like Apple to preserve users' privacy.

TOLLING & CONCEALMENT

99. The earliest Plaintiff and Class Members could have discovered the Trade Desk's conduct was shortly before the filing of this Complaint. Plaintiff became aware of the Trade Desk conduct through communications with counsel that are protected from disclosure.

100. Plaintiff and Class Members, despite their due diligence, could not have discovered the Trade Desk's conduct by virtue of how its technology works and its lack of disclosures.

101. The Trade Desk's interception of personally identifiable information and assignment of UID2 and other identifiers happens inconspicuously in the background. This process is undetectable to an ordinary person, highly technical, and prevented Plaintiff and any Class Member from uncovering it.

102. The Trade Desk had exclusive knowledge that UID2, its other identifiers, and tracking technology were tracking Plaintiff and Class Members across the internet alongside their private communications on third-party apps, websites, and other services. Similarly, the Trade Desk had exclusive knowledge that it was using this information to propagate one of the largest targeted advertising systems.

103. The Trade Desk's fraudulent conduct prevented Plaintiff and Class Members from discovering its conduct. The Trade Desk maintained a privacy policy that lacked adequate disclosures for Plaintiff and Class Members to uncover the Trade Desk ever intercepted, had, or used their data. The Trade Desk publicly held out its identifiers and technology as privacy-preserving mechanisms, even though they were not.

104. The Trade Desk was under a duty to disclose the nature and significance of its data interception and use practices—especially in light of its public statements—but did not do so. The Trade Desk is therefore estopped from relying on any statute of limitations by virtue of the discovery rule and doctrine of fraudulent concealment.

CLASS ACTION ALLEGATIONS

105. Plaintiff brings this action under Fed. R. Civ. P. 23 individually and on behalf of the following Classes:

> **Identifier Class:** All natural persons in the United States whose email address and/or phone number was intercepted to assign a UID2 or other similar identifier owned and controlled by the Trade Desk.
>
> **Communications Class**: All natural persons in the United States who had their communications with third parties intercepted or used by the Trade Desk without their consent.

106. The Classes exclude: (1) any judge presiding over this action or their immediate families; (2) the Trade Desk, its subsidiaries, affiliates, parents, successors, predecessors, and any other entity in

which the Trade Desk has a controlling interest; (3) the Trade Desk's current and former employees, officers, and directors; and (4) Plaintiff's and the Trade Desk's counsel.

107. ***Numerosity.*** While the precise size of the Classes are currently unknown to Plaintiff, each of the Classes consists of well over a million individuals and members of each of the Classes can be identified through the Trade Desk's records.

108. ***Predominant Common Questions.*** The Classes' claims present several common questions of law and fact that predominant over questions (if any) that affect individual class members. This includes:

a. Whether the Trade Desk violated Plaintiff's and the Classes' privacy rights;

b. Whether the Trade Desk engaged in unfair and deceptive conduct;

c. Whether the Trade Desk's acts and practices violate the California Invasion of Privacy Act;

d. Whether Plaintiff and Class Members are entitled to damages and/or equitable relief, including injunctive relief, restitution, and disgorgement; and

e. Whether the Trade Desk was unjustly enriched.

109. ***Typicality***. Plaintiff's claims are typical of all Class Members because they arise from the same conduct and are based on the same legal theories.

110. ***Adequate Representation***. Plaintiff will (and has) fairly and adequately represented the Classes and protected the interest of all Class Members. Plaintiff has retained competent counsel with significant experience in class action and data privacy litigation. Plaintiff and counsel have no interest that conflicts with the interests of the Classes and is not subject to any unique defenses. Plaintiff and their counsel will vigorously prosecute this action to advance the interest of the Classes and have the resources necessary to do so.

111. ***Substantial Benefits***. A class action is superior to all other possible methods to fairly and efficiently adjudicate this case and controversy, and joinder of all Class Members is impracticable. Proceeding as a class case has significant advantages to individual litigation, including: (1) comprehensive oversight by a single court, which avoids inconsistent outcomes; and (2) saving time and expense by litigating the same claims arising from the same conduct all in one action.

112. Plaintiff reserves all rights to revise or modify the class allegations based on facts and legal developments following additional investigation or discovery.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

113. California law applies to every Class Member's claims. The Trade Desk maintains its principal place of business in California and conducts substantial business in California, including the activities giving rise to Plaintiff's and Class Members' claims. California has a substantial, overriding interest in regulating the conduct of the Trade Desk under its laws. The Trade Desk's decision to reside in California and avail itself of California's laws makes the application of California law to its conduct alleged herein constitutionally permissible.

114. Under California's choice of law rules, the application of California law is appropriate because California has significant contacts to the claims and Parties in this action, California has a greater interest in applying its laws, given the Trade Desk's residency in the State and the location of the conduct at issue, over any other state.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Violation of Common Law Invasion of Privacy (Intrusion Upon Seclusion)
On Behalf of the Plaintiff and Classes

115. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

116. Intrusion upon seclusion requires pleading: (1) that the defendant intruded on a place, conversation, or matter in which plaintiff has a reasonable expectation of privacy; and (2) that the intrusion would be highly offensive to a reasonable person.

117. The Trade Desk's collection, interception, and use of Plaintiff and Class Members' phone number and email address constitutes an intentional intrusion. As does its assignment of a UID1 and UID2, the latter of which is based off these direct identifiers, to track and profile Plaintiff and Class Members based on their online activity.

118. The Trade Desk's interception and use of Plaintiff and Class Members private online communications, associated with their UID1 and/or UID2, is likewise an intentional intrusion upon Plaintiff and Class Members' solitude.

119. Plaintiff and Class Members reasonably expected their personally identifiable information, alongside their online activity, would not be intercepted or used by an unknown third-party. Email addresses and phone numbers are particularly private because they are directly identifiable, permanent identifiers. Plaintiff and Class Members reasonable expected this information would remain private and confidential and would not be intercepted or used by third parties without their consent.

120. This expectation is particularly heightened given that there were no disclosures of the Trade Desk's involvement in intercepting, processing, and using their personally identifiable information and online communications.

121. Plaintiff and Class Members did not consent to, authorize, or understand Trade Desk's interception or use of their private data.

122. The Trade Desk's conduct is highly offensive because it violates established social norms. Consumers do not expect to be surveilled whenever they use the internet, especially in light of state laws requiring companies to make adequate disclosures regarding their collection and use of data.

123. The Trade Desk's conduct is particularly offensive in light of the secretive nature in which it takes place. Plaintiff and Class Members had no way of knowing the Trade Desk collected their personally identifiable information and other online communications, and the Trade Desk did so from thousands of websites, if not more.

124. The Trade Desk's conduct caused Plaintiff and Class Members harm and injury, including a violation of their privacy interests.

125. Plaintiff and Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by the Trade Desk as a result of its intrusion upon seclusion.

126. Defendant's conduct was willful, knowing, and carried out with a conscious disregard for Plaintiff's rights, Plaintiff are entitled to punitive and exemplary damages.

127. Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

SECOND CAUSE OF ACTION

Violation of Article I, Section 1 of the California Constitution (Invasion of Privacy)
On Behalf of the Plaintiff and Classes

128. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

129. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

130. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

131. The right to privacy in California's constitution creates a right of action against private and government entities.

132. Plaintiff and Class Members have and continue to have a reasonable expectation of privacy in their personal information, identities, and private data, pursuant to Article I, Section I of the California Constitution.

133. The identifiable and private information the Trade Desk intercepted, stored, and used without Plaintiff and Class Members' consent was used to track them consistently, and persistently, across internet-connected services and to serve targeted advertisements. The manner in which the Trade Desk intercepted this information defeated established privacy-mechanisms and social norms.

134. This conduct constitutes an extremely serious invasion of privacy that would be highly offensive to a reasonable person. Reasonable individuals do not expect that there is an entity intercepting and monitoring all of their online activity, let alone using it for profit.

135. The Trade Desk's conduct violated the privacy of hundreds of thousands (if not millions) of Class Members, including Plaintiff. The Trade Desk did not have consent to intercept this information, let alone use it.

136. Plaintiff and Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by the Trade Desk as a result of its intrusion upon seclusion.

137. Defendant's conduct was willful, knowing, and carried out with a conscious disregard for Plaintiff's rights, Plaintiff is entitled to punitive and exemplary damages.

138. Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

THIRD CAUSE OF ACTION
Violation of the California Invasion of Privacy Act ("CIPA")
Cal. Penal Code § 631
On Behalf of the Plaintiff and Classes

139. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

140. CIPA § 631 prohibits any person who uses a "machine, instrument, contrivance" or in "any other manner": (1) intentionally taps or makes an unauthorized connection with "any telegraph or telephone wire, line, cable, or instrument"; (2) willfully and without consent of "all parties to the communication" or in "any unauthorized manner" reads or "attempts to read" or "learns 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" California; (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way" information so obtained; or (4) from aiding, agreeing, employing, or conspiring 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."

141. The Trade Desk is a person under CIPA § 631.

142. The Trade Desk maintains its principal place of business in California, which is where it designed, created, conspired, and effectuated the interception and use of Plaintiff and Class Members' personally identifiable information and private communications.

143. The Trade Desk's technology (e.g., the Universal Pixel, UID2 framework, etc.), and Plaintiff's and Class Members' computers, mobile devices, and connected TVs, are a "machine, instrument, contrivance, or . . . other manner" under CIPA § 631.

144. At all relevant times, the Trade Desk used its technology to make unauthorized connections with the lines of communication and instruments used by Plaintiff and Class Members to access online services without the consent of all parties to those communications.

145. The Trade Desk willfully, and without consent, read or attempted to read, or learn the contents and meaning of, Plaintiff and Class Members' communications with online services while those communications were in transmit or passing over a wire, line, or cable, or were being sent or received within California through the Universal Pixel and its UID1/2 framework, as described herein. This interception happens prior to or at the same time they would be received by the intended recipient.

146. The Trade Desk used, and attempted to use, these identifiable, private communications for its own benefit, including targeted advertising as described herein.

147. The Trade Desk also aided, agreed with, employed, and conspired with Private Operators and advertising entities to intercept and use this data for profit.

148. The interception and use of Plaintiff's and Class Members' communications was without authorization or consent from Plaintiff and Class Members.

149. Plaintiff and Class Members have been harmed as a result of the Trade Desk's conduct. Their private data has been intercepted, viewed, and used for targeted advertising and has not been destroyed. Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

150. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

FOURTH CAUSE OF ACTION
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 632
On Behalf of the Plaintiff and Classes

151. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

152. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication[.]"

153. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

154. Plaintiff's and Class Members' communications to online services are confidential communications for purposes of § 632, because Plaintiff and Class Members had an objectively reasonable expectation of privacy in this data.

155. Plaintiff and Class Members expected their communications would not be shared with the Trade Desk, as there were no disclosures that the Trade Desk would secretly eavesdrop upon or record their information and communications.

156. The Trade Desk's Universal Pixel and UID1/2 framework are electronic amplifying or recording devices for purposes of § 632.

157. By contemporaneously intercepting and recording Plaintiff's and Class Members' confidential and identifiable communications to online services through this technology, the Trade Desk eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

158. At no time did Plaintiff or Class Members consent to the Trade Desk's conduct, nor could they reasonably expect that their communications with online services would be overheard and recorded by the Trade Desk.

159. The Trade Desk utilizes these private communications for their own benefit, including to serve targeted advertisements and develop user profiles.

160. Plaintiff and Class Members have been harmed as a result of the Trade Desk's conduct. Their private data has been intercepted, viewed, and used for targeted advertising and has not been destroyed. Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

161. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

FIFTH CAUSE OF ACTION
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 638.50 & 638.51
On Behalf of the Plaintiff and Classes

162. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

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

164. Separately, CIPA § 638.50(c) defines a "[t]rap and trace device" as 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."

165. CIPA § 638.51 prohibits a person from installing either a pen register or trap and trace device without a court order.

166. The Trade Desk is a person under CIPA § 638.51.

167. The Trade Desk implemented and installed the Universal Pixel and UID1/2 framework—which are pen registers and/or trap and trace devices—on Plaintiff's and Class Members' devices and browsers.

168. These processes captured "routing, addressing, or signaling information" because they intercept: (1) users' directly identifiable information, either email addresses or phone numbers; (2) existing UID2s (either in raw or tokenized form) keyed off users' email addresses or phone numbers; (3) UID1, which is a persistent cookie used to track users' across the internet; (4) the "adv" which is a parameter that identifies the "advertiser" whose website is visited and uses the Trade Desk's offending

software/processed; and (5) the destination URL (e.g., the domain of the webpages or other online services the user visited).

169. The Trade Desk was not authorized by any court order to use a pen register or trap and trace device to record or capture Plaintiff's and Class Members' routing, addressing, or signaling information.

170. Plaintiff and Class Members did not consent to the Trade Desk's installation of a pen register or trap and trace device on their devices and browsers.

171. Plaintiff and Class Members have been harmed as a result of the Trade Desk's conduct. The Trade Desk did not have authorization to use pen registers and/or trap and trace devices to surveille and identify Plaintiff and Class Members or other routing, addressing, and signaling information revealing who the intended recipients of their communications were.

172. Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

173. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

SIXTH CAUSE OF ACTION
Violation of the Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502 ("CDAFA")
On Behalf of the Plaintiff and Classes

174. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

175. The California Legislature enacted the CDAFA to "expand the degree of protection afforded . . . from tampering, interference, damage, and unauthorized access to [(including the extraction of data from)] lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the

integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals . . .” Cal. Penal Code § 502(a).

176. Plaintiff’s and Class Members’ devices on which Trade Desk’s Tracking Technology is installed, including their computers, smart phones, and tablets, constitute “Computer system[s]” within the meaning of the CDAFA. *Id.* § 502(b)(5).

177. The data that Trade Desk accessed and collected from Plaintiff’s and Class Members’ devices constitute “Data” within the meaning of the CDAFA. *Id.* § 502(b)(8).

178. Defendant Trade Desk violated § 502(c)(1) of the CDAFA by knowingly accessing and using without permission Plaintiff’s and Class Members’ devices in order to wrongfully obtain and use their personal data, in violation of users’ reasonable expectations of privacy in their devices and data.

179. Defendant Trade Desk violated § 502(c)(2) of the CDAFA by knowingly and without permission taking, copying, and making use of Plaintiff’s and the Class Members’ personally identifiable information from their devices.

180. Defendant Trade Desk’s Tracking Technology incorporated on Plaintiff’s and the Class Members’ devices constitute “computer services” within the meaning of the CDAFA. Defendant Trade Desk violated § 502(c)(3) by knowingly and without permission using those computer services, and/or causing them to be used. Defendant Trade Desk violated § 502(c)(7) by knowingly and without permission accessing those devices, and/or causing them to be accessed.

181. Defendant Trade Desk violated §§ 502(c)(6) and (c)(13) of the CDAFA by knowingly, and without permission from Plaintiff and the Class Members, providing and/or assisting in providing advertisers and ads publishers the ability to access Plaintiff’s and the Class Members’ personal data via its Tracking Technology.

182. Under § 502(b)(12) of the CDAFA a “Computer contaminant” is defined as “any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information.” Defendants Trade Desk violated § 502(c)(8) by knowingly and without permission introducing a computer contaminant via its Tracking Technology incorporated on Plaintiff’s and the Class Members’

devices, which intercepted their personal data. As described *supra*, the Tracking Technology is deeply hidden; Plaintiff and Class Members had no way to remove it or opt out of its functionality.

183. Plaintiff and Class Members suffered damage and loss as a result of the Trade Desk's conduct. The Trade Desk's practices have deprived Plaintiff and the Class Members of control over their valuable property (namely, their sensitive personal data), the ability to receive compensation for that data, and the ability to withhold their data for sale.

184. Plaintiff and the Class Members seek compensatory damages in accordance with CDAFA § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

185. Plaintiff and Class Members have also suffered irreparable and incalculable harm and injuries from the Trade Desk's violations. The harm will continue unless the Trade Desk is enjoined from further violations of this section. Plaintiff and Class Members have no adequate remedy at law.

186. Plaintiff and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because the Trade Desk's violations were willful and, upon information and belief, the Trade Desk is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294. Plaintiff and the Class Members are also entitled to recover their reasonable attorneys' fees under § 502(e)(2).

SEVENTH CAUSE OF ACTION
Unjust Enrichment
On Behalf of the Plaintiff and Classes

187. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

188. The Trade Desk receives benefits from Plaintiff and Class Members in the form of their personally identifiable information and private online communications. The Trade Desk acquired this information without Plaintiff's and Class Members' authorization and without providing corresponding compensation.

189. The Trade Desk acquired and used this private data for its own benefit, including tangible economic benefits from companies that used the Trade Desk for targeted advertising.

190. Had Plaintiff and Class Members known of the Trade Desk's misconduct, they would not have agreed the Trade Desk could acquire and use their private data.

191. The Trade Desk unjustly retained these benefits at the expense of Plaintiff and Class Members. Plaintiff and Class Members were harmed by this conduct and were not provided any commensurate compensation.

192. The benefits the Trade Desk received and derived from Plaintiff and Class Members' private data rightly belong to Plaintiff and Class Members. It is inequitable under unjust enrichment principles for the Trade Desk to retain the profits and other intangible benefits they derived through its wrongful conduct.

193. The Trade Desk should be compelled to disgorge these profits and other inequitable proceeds in a common fund for the benefit of Plaintiff and Class Members.

EIGHTH CAUSE OF ACTION
Injunctive Relief
On Behalf of the Plaintiff and Classes

194. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

195. The Trade Desk's conduct has and continues to cause harm to Plaintiff and Class Members' privacy and autonomy, as it continues to store unique persistent identifiers, as well as the private contents of their communications, on its own systems. The Trade Desk routinely uses this information for targeted advertising.

196. Accordingly, Plaintiff and Class Members seek injunctive relief, including an order permanently restraining the Trade Desk from continuing to use and store this information without consent and/or a court order, and requiring the Trade Desk to delete this information from its systems.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the putative Class requests the Court enter an Order:

a. Certifying the Classes and appointing Plaintiff as Class Representative;

b. Finding the Trade Desk's conduct unlawful;

c. Awarding injunctive and other equitable relief as is just and proper;

d. Awarding Plaintiff and the Classes statutory, actual, compensatory, punitive, nominal, and other damages, as well as restitution and/or disgorgement of unjust and unlawful profits;

e. Awarding pre-judgment and post-judgment interest;

f. Awarding reasonable attorneys' fees, costs, and expenses; and

g. Granting any other relied as the Court sees just and proper.

Dated: April 7, 2025

/s/ James Wagstaffe

James M. Wagstaffe, Esq.
ADAMSKI MOROSKI MADDEN CUMBERLAND & GREEN LLP
P.O. Box 3835
San Luis Obispo, CA 93403-3835
Tel: 805-543-0990
Fax: 805-543-0980

Christian Levis (*pro hac vice* forthcoming)
clevis@lowey.com
Amanda Fiorilla (*pro hac vice* forthcoming)
afiorilla@lowey.com
Rachel Kesten (*pro hac vice* forthcoming)
rkesten@lowey.com
Yuanchen Lu (*pro hac vice* forthcoming)
ylu@lowey.com
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035