Lesley Weaver (Cal. Bar No.191305)
Matthew S. Melamed (Cal. Bar No. 260272)
Anne K. Davis (Cal. Bar No. 267909)
Angelica M. Ornelas (Cal. Bar No. 285929)
Joshua D. Samra (Cal. Bar No. 313050)
BLEICHMAR FONTI & AULD LLP
555 12th Street, Suite 1600
Oakland, CA 94607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com
mmelamed@bfalaw.com
adavis@bfalaw.com
aornelas@bfalaw.com
jsamra@bfalaw.com

Elizabeth C. Pritzker (Cal. Bar No. 146267)
Jonathan K. Levine (Cal Bar No. 220289)
Caroline C. Corbitt (Cal Bar No. 305492)
PRITZKER LEVINE LLP
1900 Powell Street, Suite 450
Emeryville, CA 94608
Tel.: (415) 692-0772
Fax: (415) 366-6110
ecp@pritzkerlevine.com
jkl@pritzkerlevine.com
ccc@pritzkerlevine.com

Attorneys for Plaintiffs

Mitchell M. Breit (*pro hac vice* to be sought)
Jason 'Jay' Barnes (*pro hac vice* to be sought)
An Truong (*pro hac vice* to be sought)
Eric Johnson (*pro hac vice* to be sought)
SIMMONS HANLY CONROY LLC
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
Fax: (212) 213-5949
mbreit@simmonsfirm.com
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

BENJAMIN HEWITT and KIMBERLEY WOODRUFF, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

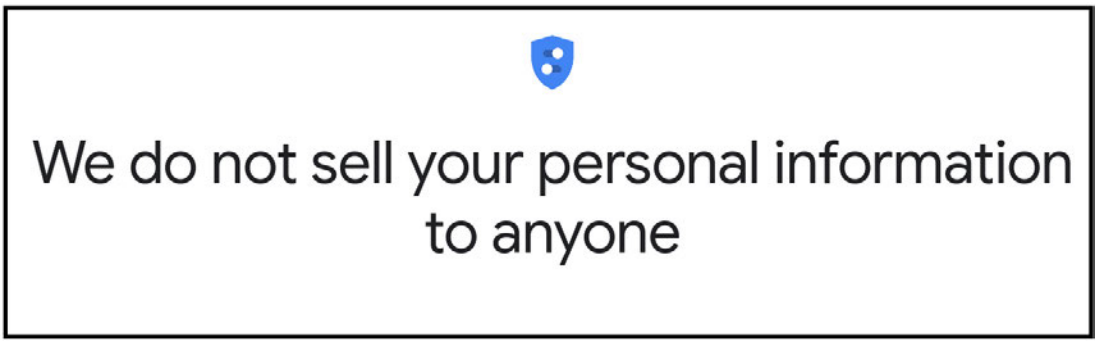
TABLE OF EXHIBITS

EX.	DOCUMENT DESCRIPTION
1	Documents Constituting the Relevant Contract from June 28, 2016 to Present
2	Google Terms of Service dated April 14, 2014
3	Google Terms of Service dated Oct. 25, 2017
4	Google Terms of Service dated March 31, 2020
5	*How our business works*, Google, https://about.google/intl/en_US/how-our-business-works/ (last visited Mar. 26, 2021)
6	Google Privacy Policy dated June 28, 2016
7	Google Privacy Policy dated Aug. 29, 2016
8	Google Privacy Policy dated March 1, 2017
9	Google Privacy Policy dated April 17, 2017
10	Google Privacy Policy dated Oct. 2, 2017
11	Google Privacy Policy dated Dec. 18, 2017
12	Google Privacy Policy dated May 25, 2018
13	Google Privacy Policy dated Jan. 22, 2019
14	Google Privacy Policy dated Oct. 15, 2019
15	Google Privacy Policy dated Dec. 19, 2019
16	Google Privacy Policy dated Mar. 31, 2020
17	Google Privacy Policy dated July 1, 2020
18	Google Privacy Policy dated Aug. 28, 2020
19	Google Privacy Policy dated Sept. 30, 2020
20	Google Privacy Policy dated Feb. 4, 2021
21	*Who are Google's Partners?*, Google, https://policies.google.com/privacy/google-partners?hl=en-US (last visited Mar. 25, 2021)
22	*Personalized Advertising*, Google, https://support.google.com/adspolicy/answer/143465 (last visited Mar. 25, 2021)

EX.	DOCUMENT DESCRIPTION
23	*We do not sell your personal information to anyone*, Google, https://safety.google/intl/en_ca/privacy/ads-and-data/ (last visited Mar. 25, 2021)
24	*Your privacy is protected by responsible data practices*, Google, https://safety.google/intl/en_us/privacy/data/ (last visited Mar. 25, 2021)
25	Pichai, Sundar (May 7, 2019), *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, The New York Times (emphasis added), available at: https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html
26	Google AdWords API: VERTICALS https://developers.google.com/adwords/api/docs/appendix/verticals (last visited Mar. 24, 2021)
27	Google Example OpenRTB Protobuf for Web video Real-Time Bidding: Pregnancy and Maternity Vertical, https://developers.google.com/authorized-buyers/rtb/request-guide#openrtb-protobuf_6 (last visited January 22, 2021)
28	Google Example OpenRTB Protobuf for "App native" Real-Time Bidding: OBGYN Vertical, https://developers.google.com/authorized-buyers/rtb/request-guide#openrtb-protobuf_6 (last visited January 22, 2021)

I. INTRODUCTION

1. Through its various consumer-facing products and services – and its business advertising and surveillance tools – Google amasses data about billions of people for the purpose of creating detailed dossiers about them in furtherance of targeted advertising. Recognizing that American consumers have significant privacy concerns, however, Google makes two "unequivocal" promises to users who sign up for Google's services: (1) "Google will never sell any personal information to third parties;" and (2) "you get to decide how your information is used."[1] Google also promises that it will not use certain sensitive information for advertising purposes.



2. Google breaks these promises billions of times every day.

3. This Complaint identifies how Google actively sells and shares consumers' personal information with thousands of entities, ranging from advertisers to publishers to hedge funds to political campaigns and even to the government, through its Google Real-Time Bidding system. The personal information that Google sells, shares and uses includes the very sensitive information Google promised it would not use for advertising purposes. These practices are not disclosed to consumers.

4. This case is brought on behalf of all Google account holders whose personal information is sold and disseminated by Google to thousands of companies through Google's proprietary advertising auction process effectuated through real-time bidding ("RTB") auctions.

5. Regulators have described RTB as follows:

> RTB is the process by which the digital ads we see every day are curated. For each ad, an auction takes place milliseconds before it is

[1] Pichai, Sundar (May 7, 2019), *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good,* The New York Times, available at https://www.nytimes.com/2019/05/07/pinion/google-sundar-pichai-privacy.html (attached as Exhibit 25).

> shown in an app or browser. The hundreds of participants in these auctions receive sensitive information about the potential recipient of the ad—device identifiers and cookies, location data, IP addresses, and unique demographic and biometric information such as age and gender. Hundreds of potential bidders receive this information, even though only one—the auction winner—will use it to deliver an advertisement.
>
> Few Americans realize that companies are siphoning off and storing that "bidstream" data to compile exhaustive dossiers about them. These dossiers include their web browsing, location, and other data, which are then sold by data brokers to hedge funds, political campaigns, and even to the government without court orders.[2]

6. Google runs the world's largest RTB auction (the "Google RTB"). In the Google RTB, Google solicits participants to bid on sending an ad to a specific individual (the "Target"). Google provides highly specific information about the Target in the Bid Request provided to auction participants, including data that identifies the individual person being targeted through unique identifiers, device identifiers and IP addresses, among other information. The collected data provided about the Target to auction participants is called "Bidstream Data."

7. Auction participants receive the information and compete for ad space to send a message to the Target at a specific price. The winning bidder pays Google for the ad placement with currency. But all auction participants, even those who do not win and those who do not submit a bid, are able to collect Bidstream Data on the Target. Such "non-winning" auction participants include not just auction participants who engage in the RTB process with the intent of competing to fill the ad space, but also pure "Surveillance Participants" – participants that have no interest in filling the ad space but who participate in Google's RTB for the sole purpose of gaining access to the Target's Bidstream Data. Even though they do not bid, the Surveillance Participants' presence drives interest and encourages competitive bids, which increases the reach and profitability of Google RTB.

8. The Google RTB process takes place in fewer than 100 milliseconds, faster than the blink of an eye.

---

[2] Senator Ron Wyden (Oregon), et al. (July 31, 2020), Letter to Hon. Joseph J. Simmons, Chairman of the Federal Trade Commission (FTC) urging FTC investigation of RTB ("Wyden FTC Letter"), available at https://www.wyden.senate.gov/imo/media/doc/073120%20Wyden%20Cassidy%20Led%20FTC%20Investigation%20letter.pdf

9. Google's ability to provide a rich and highly personalized set of Bidstream Data for each Target is unprecedented and is the primary source of Google's massive revenues. Google is a consumer data powerhouse unmatched in human history. Google operates the world's largest search engine (Google.com), web-browser (Chrome), email service (Gmail), Internet video service (YouTube), mobile phone operating system (Android), and mapping service (Google Maps). Google also operates large consumer services in app sales (Google Play), document processing (Google Docs), scheduling (Google Calendars), storage (Google Drive), instant messaging (Google Chat), travel planning (Google Flights), fitness (Google Fit), videoconferencing (Google Meet), payment services (Google Pay), smartphone hardware (Google Pixel), laptop hardware (Chromebooks), and broadcast television (YouTube TV).

10. Through these services, Google surreptitiously observes, collects, and analyzes real-time information about everyone engaging on those platforms. This includes collecting and selling information about activity users could not expect to be sold. Google's purpose is to build massive repositories of the most current information available about the people using its services to sell it to Google's partners. But because transparency about those practices would lead to less user engagement on those platforms, which in turn would impede its ability to maximize targeted ad revenues, Google fails to make accurate, transparent disclosures about those practices to its account holders.

11. Instead, Google promises its account holders privacy and control. Any consumer can sign up for a Google Account by clicking a button assenting to the terms of service that Google has unilaterally drafted. In that contract, Google makes the following promises:

a. "You get to decide how your information is used." Ex. 25 at 1.

b. "We don't sell your personal information to anyone." Ex. 5 at 1.

c. "Advertisers do not pay us for personal information." Ex. 5 at 1.

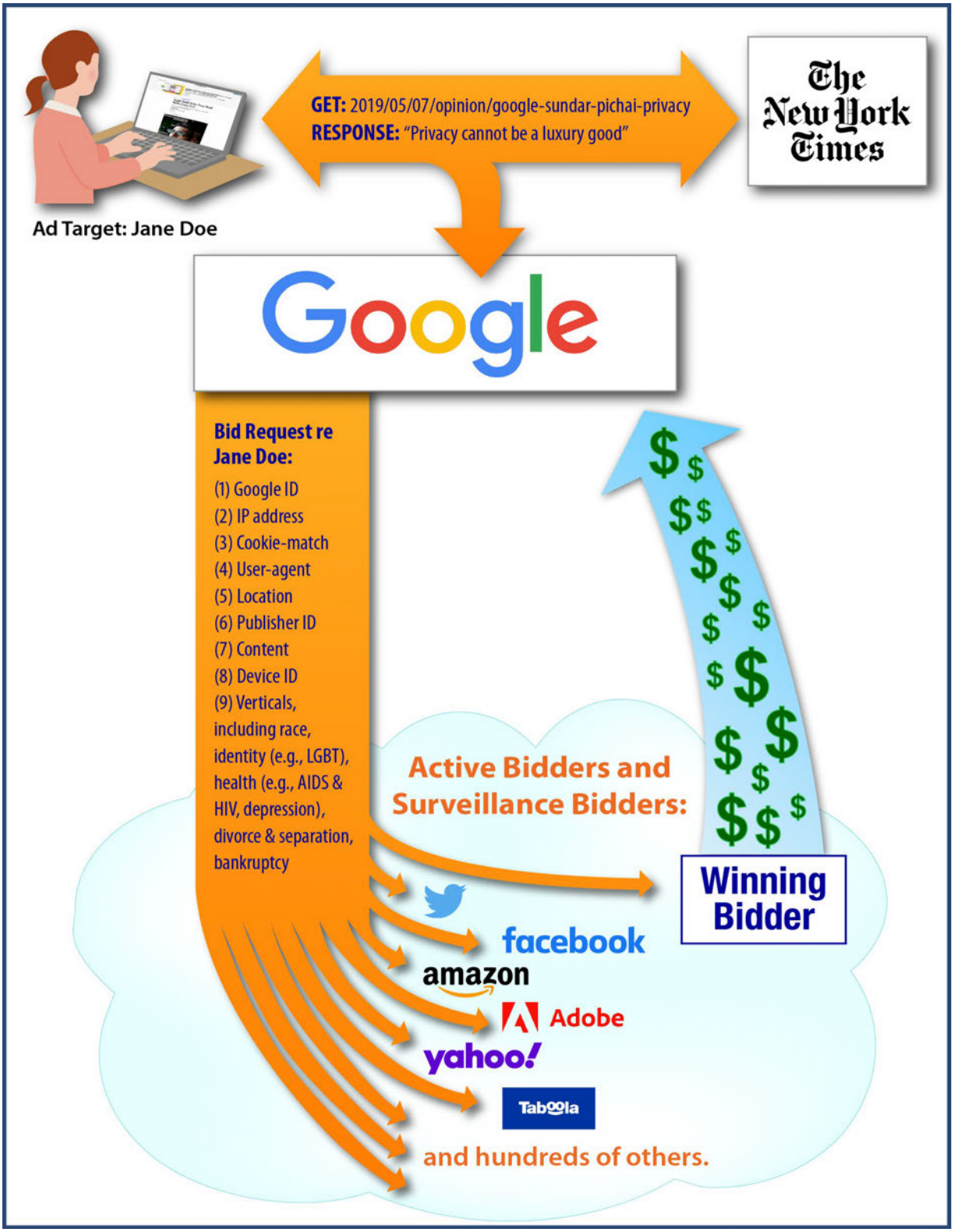
d. "We don't share information that personally identifies you with advertisers." *E.g.* Ex. 20 at 6.

e. "We also never use … sensitive information like race, religion, or sexual orientation, to personalize ads to you." Ex. 5 at 1.

f. "We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health." *E.g.* Ex. 20 at 6.

12. Google does not honor these terms. Without telling its account holders, Google automatically and invisibly sells Bidstream Data about them to thousands of different participants on the Google RTB billions of times every day. The Bidstream Data that Google sells and discloses to thousands of Google RTB participants identifies individual account holders, their devices, and their locations; the specific content of their Internet communications; and even highly personal information about their race, religion, sexual orientation, and health.

13. The Google RTB system may be illustrated as follows:



14. Contrary to Google's promises, Bidstream Data is not anonymized. It includes:

a. A Google ID for each account holder;

b. The account holder's IP address;

c. A cookie-matching service that helps the recipient match the account holder's personal information up with other personal information that the recipient has on the account holder;

d. The account holder's User-Agent information;

e. The Publisher ID of the website in question;

f. The content of the URL for the webpage where the ad will be placed;

g. The account holder's unique device identifier; and

h. "Vertical" interests associated with the bid that include interests relating to race, religion, health, and sexual orientation.

15. The "verticals" included in Bidstream Data sold and disclosed on Google RTB categorize Google's account holders into targetable interests. Google runs algorithms across the massive repositories of data it acquires about account holders and sorts them into more than 5,000 consumer categories (segments) and subcategories (verticals). According to Google's own description of the segments and verticals, these categories include:

a. In the Health segment, verticals include AIDS & HIV, Depression, STDs, and Drug & Alcohol Treatment. Ex. 24 at 14.

b. In the Religion segment, verticals include Buddhism, Christianity, Hinduism, Islam, and Judaism. *Id.* at 21.

c. In the Identity segment, verticals include African-Americans, Jewish Culture, and LGBT. *Id.*

d. In the Finance segment, verticals include Debt Collection and Short-Term Loans and Cash. *Id.* at 11-12.

e. Other verticals include Troubled Relationships, Divorce & Separation, and Bankruptcy. *Id.* at 21.

16. These "verticals" exemplify Google's use of the information it collects about account holders' activities and its ability to take that information and infer personal and sensitive characteristics. Google then packages account holders into narrowly drawn, targetable categories. That is, the Bidstream Data that Google provides to Google RTB participants is drawn from the extensive profile Google has built on the Target. This data set includes information based on Google's distillation of both public and highly private data points and inferences. Google's

Bidstream Data on Targets is so compelling that publishers are incentivized to choose Google RTB over other services to place their messages, and bidders in Google RTB will offer to pay premium dollars for the information. And all participants, including Surveillance Participants, can keep the Bidstream Data for each Target, which encourages Surveillance Participants to participate even if they do not wish to buy the ad space. But the consumers themselves do not even know that these categories exist, let alone that Google has placed them into one of these categories.

17. Data included in Bidstream Data constitutes "personal information" under California law. Google adopts California law in its contract with account holders. California law defines "personal information" to include any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." California law also provides a non-exhaustive list of "personal information," which includes unique personal identifiers, online identifiers, IP addresses, email addresses, account names, characteristics of protected classifications under California or federal law, purchase history or consideration, Internet or other electronic network activity (including browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement), geolocation data, employment-related information, education information, and "inferences drawn … to create a profile about a consumer reflect the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." Cal. Civ. Code § 1798.140(o)(1). Thus, the information Google sells and discloses as part of a Target's Bidstream Data includes personal information under California law.

18. The exchange of Bidstream Data for auction participation constitutes a "sale" of "personal information." California law defines a sale of personal information as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating … by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." Cal. Civ. Code § 1798.140(t)(1).

19. Google's dissemination and sale of the type of Bidstream Data available in Google RTB violates Google's express contractual promises to its account holders.

20. It also violates laws prohibiting Google from selling account holders' personal and/or sensitive information, including (and especially) when it sells and discloses such information for the purpose of targeting them.

21. Google does not disclose to its account holders its creation and use of massive data sets to profile them specifically (and identifiably) in these auctions, and it cannot plausibly or credibly claim it has account holders' consent for this use of their data and information. None of the categories of information in Bidstream Data are identified in any of the many policies and terms of service Google presents to account holders. Indeed, the success of Google's RTB process is a function, in part, of the fact that account holders – the Targets for ad placements – are unaware that information drawn from their activities wholly unrelated to any bid are incorporated into what is presented to them in targeted ads milliseconds later.

22. "We also never use your emails, documents, photos, or sensitive information like race, religion, or sexual orientation, to personalize ads to you," Google tells account holders. Ex. 5 at 2. But that is precisely what Google does. Google RTB bidders specifically seek to stimulate response in the Target based on the way Google slots the Target into verticals and segments concerning, among other things, the Target's race, religion, and sexual orientation.

23. The breadth of Google's privacy violations is staggering. Plaintiffs engaged an expert, Professor Christo Wilson, to help identify the scope of Google's dissemination of Bidstream Data on individual Targets. Professor Wilson identified 1.3 million separate publishers participating in Google's ad systems. Each of those publishers is a potential recipient of Google RTB Bidstream Data, including the personal information Google tells account holders it will not share.

24. Once a Target's Bidstream Data is disseminated by Google, the data is not recoverable.

25. Because Google account holders are not informed about this dissemination of their personal information – indeed, they are told the opposite – they cannot exercise reasonable

judgment to defend themselves against the insidious, pervasive, and highly personal ways Google has used and continues to use data Google has about them to make money for itself. Nor can account holders exercise reasonable judgment to defend themselves against winning bidders that are targeting them individually, or Surveillance Participants that use Google RTB to build their own data profiles on account holders.

26. In July 2020, Senator Ron Wyden and nine other members of Congress wrote a letter to the Federal Trade Commission explaining the privacy dangers of RTB systems. The letter explained:

> Unregulated data brokers have access to bidstream data and are using it in outrageous ways that violate Americans' privacy. For example, media reports recently revealed that Mobilewalla, a data broker and a buyer of bidstream data, used location and inferred race data to profile participants in recent Black Lives Matter protests. Moreover, Mobilewalla's CEO revealed, in a podcast recorded in 2017, that his company tracked Americans who visited places of worship and then built religious profiles based on that information.
>
> The identity of the companies that are selling bidstream data to Mobilewalla and countless other data brokers remains unknown. However, according to major publishers, companies are participating in RTB auctions solely to siphon off bidstream data, without ever intending to win the auction and deliver an ad. …
>
> Americans never agreed to be tracked and have their sensitive information sold to anyone with a checkbook. … This outrageous privacy violation must be stopped and the companies that are trafficking in Americans' illicitly obtained private data should be shut down.[3]

27. Plaintiffs bring this class action on behalf of themselves and all Google account holders in United States whose personal information was sold or otherwise disclosed by Google without their authorization, and assert claims for breach of contract, violations of statutory and common law, and equitable claims against Google for compensatory damages, including statutory damages where available, unjust enrichment, punitive damages, injunctive relief, and all other remedies permitted by law.

[3] Wyden FTC Letter.

II. JURISDICTION, VENUE, AND ASSIGNMENT

28. This Court has personal jurisdiction over Defendant Google LLC ("Defendant" or "Google") because it is headquartered in this District. Google also concedes personal jurisdiction in its current and prior Google Terms of Service. *See* Exhibits 2 through 4.

29. Venue is proper in this District because Google is headquartered in this District and because its current and prior Terms of Service purport to bind Plaintiffs to bring disputes in this District. *See id.*

30. Assignment of this case to the San Jose Division is proper pursuant to Civil Local Rule 3-2(c)(e) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in Santa Clara County, California.

31. This Court has subject matter jurisdiction over the federal claims in this action. *Infra* Counts Nine, Ten, Eleven, and Twelve.

32. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, and at least one member of the class is a citizen of a state other than the state in which Google maintains its headquarters (California) and in which it is incorporated (Delaware).

33. This Court has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

III. PARTIES

34. Plaintiff Benjamin Hewitt is an adult domiciled in California. Plaintiff Hewitt is a Google account holder who has used the Internet, including websites from which Google sold and shared account holder information without authorization, as alleged herein. Plaintiff Hewitt has used the Chrome web browser. In order to become a Google account holder, Plaintiff Hewitt was required to indicate he agreed to uniform conditions drafted and set forth exclusively by Google that govern the relationship between him and Google.

35. Plaintiff Kimberley Woodruff is an adult domiciled in Missouri. Plaintiff Woodruff is a Google account holder who has used the Internet, including websites from which Google sold and shared account holder information without authorization, as alleged herein. Plaintiff Woodruff has used the Chrome web browser. In order to become a Google account holder, Plaintiff Woodruff was required to indicate she agreed to uniform conditions drafted and set forth exclusively by Google that govern the relationship between her and Google.

36. Because of the ubiquity of Google's advertising services to businesses and its surveillance technologies, it is practically impossible for any American to use the Internet without their personal information being subject to Google RTB. As alleged below, nearly 1.3 million different publishers or brokers for publishers are identified by Google as being involved on the supply side in the Google RTB system.

37. On information and belief, like millions of other Americans, Google has sold and shared Plaintiffs' personal information through Google RTB. Plaintiff Hewitt frequently uses Chrome to request, obtain and watch audio-visual materials, including materials from publishers for which he is a subscriber. On information and belief, like millions of Americans, Google has sold and shared information about the video materials Plaintiff Hewitt receives and obtains on Chrome through Google's RTB auctions without his express written consent.

38. Defendant Google is a Delaware Limited Liability Company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, whose membership interests are entirely held by its parent holding company, Alphabet, Inc. ("Alphabet"), headquartered at the same address. Alphabet trades under the stock trading symbols GOOG and GOOGL. Alphabet generates revenues primarily by delivering targeted online advertising through the Google subsidiary. All operations relevant to this complaint are run by Google.

IV. FACTUAL ALLEGATIONS

A. The Operative Terms of Service Between Google and Google Account Holders Repeatedly and Uniformly Promise that Google Will Not Sell Account Holders' Personal Information to Google RTB Participants

39. A Google Account gives a user access to Google products.[4] The user, in turn becomes a Google account holder (the "Account Holder").

40. Google requires an Account Holder to indicate they agree to the Google Terms of Service (the "Terms of Service").

41. The Terms of Service are drafted exclusively by Google.

42. Though the Terms of Service at issue are materially identical throughout the Class Period, the manner by which they were presented to persons creating a Google Account shifted slightly over the relevant time period. All versions of the Terms of Service contain the following assertions material to the claims asserted herein:

1. The Terms of Service Provide That California Law Governs

43. At all times relevant to Plaintiffs' allegations, the Terms of Service designated California law as governing law.

44. Google is bound by the California's definition of "personal information."

45. California law defines personal information as "information that identifies, relates to, describes, ***is reasonably capable of being associated with***, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(o)(1) (emphasis added).

46. California law also provides a non-exhaustive list of information deemed to be personal information: "Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

[4] Google Account Help, Create A Google Account, https://support.google.com/accounts/answer/27441?hl=en&ref_topic=3382296.

a. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

b. Any categories of personal information described in subdivision (e) of Section 1798.80.

c. Characteristics of protected classifications under California or federal law.

d. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

e. Biometric information.

f. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

g. Geolocation data.

h. Audio, electronic, visual, thermal, olfactory, or similar information.

i. Professional or employment-related information.

j. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232(g); 34 C.F.R. Part 99).

k. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

Id. (emphasis added).

2. The Terms of Service State Google Will Not Sell or Share Personal Information

47. Since March 31, 2020, the Terms of Service have stated, "You have no obligation to provide any content to our services and you're free to choose the content that you want to provide." Ex. 4 at 5.

48. The second paragraph of the Terms of Service provides:

> These Terms of Service reflect the way Google's business works, the laws that apply to our company, and certain things we've always believed to be true. As a result, these Terms of Service help define Google's relationship with you as you interact with our services. For example, these terms include the following topic headings:
>
> - What you can expect from us, which describes how we provide and develop our services
> - What we expect from you, which establishes certain rules for using our services
> - Content in Google services, which describes the intellectual property rights to the content you find in our services — whether that content belongs to you, Google, or others
> - In case of problems or disagreements, which describes other legal rights you have, and what to expect in case someone violates these terms
>
> Understanding these terms is important because, by using our services, you're agreeing to these terms.

49. The reference and hyperlink to "the way Google's business works" takes the Account Holder to Google's "How our business works" page, thereby incorporating that linked document into the Terms of Service. On the very first page of that linked document, in large type, Google declares: "We don't sell your personal information to anyone." Google also states, "[W]e never sell your personal information to anyone[.]"[5]

> ## We don't sell your personal information to anyone
>
> We use your personal information to make our products more helpful to you. It's how we can autocomplete your searches, get you home faster with Maps, or show you more useful ads based on your interests. But we never sell your personal information to anyone and you can use many of our products without signing in or saving any personal information at all.

50. The "the way Google's business works" page further promises:[6]

a. "Advertisers do not pay us for personal information[.]"

b. "[W]e never share that information with advertisers, unless you ask us to."

[5] Ex. 5 at 1-2.

[6] *Id.* at 1-2.

c. "We also never use your emails, documents, photos, or sensitive information like race, religion, or sexual orientation, to personalize ads to you."

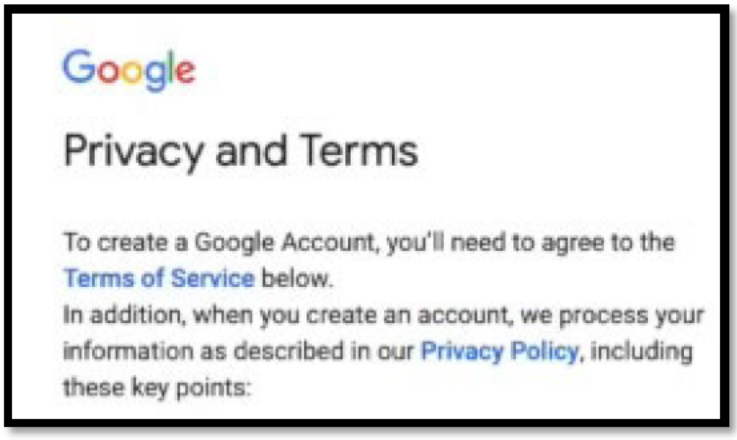
d. "We share reports with our advertisers to help them understand the performance of their ads, but we do so without revealing any of your personal information."

e. "At every point in the process of showing you ads, we keep your personal information protected with industry-leading security technologies."

3. The Google Privacy Policy Promises Not to Sell or Share Personal Information

51. Prior to around May 2018, Account Holders who created a Google Account were required to agree to both the Terms of Service and the Google Privacy Policy (the "Privacy Policy").

52. From around May 2018 to present, Account Holders who created a Google Account were required to agree only to the Terms of Service. While Account Holders were not required to agree to the Privacy Policy during this period, the Google Account creation process included a link (see below) to the Privacy Policy as a guide to how Google would "process your information."[7] As described further below, the Privacy Policy during this time contained repeated assurances and representations from Google regarding how Google would process Account Holders' information.



53. From March 31, 2020 to present, the Terms of Service refer to the Privacy Policy, but state that the Privacy Policy is "not part of these terms." Ex. 4 at 1. During this time period, the Terms of Service expressly state that the "Terms of Service reflect the way Google's business

[7] *See, e.g.*, Tom Leeman, *How to create a Google Account*, YouTube (Feb. 2, 2020) https://www.youtube.com/watch?v=ArZpwBl_z10 (at 4:40-4:45).

works [hyperlink]." *Id.* The hyperlink takes an Account Holder to the "How our business works" webpage, thereby incorporating the terms set forth on that webpage into the Terms of Service. Accordingly, as of March 31, 2020, the contract between the Parties consisted of the Terms of Service and the Google "How our business works" webpage (discussed above).

54. Like the Terms of Service, the Privacy Policy made promises to Account Holders throughout the Class Period regarding the protection of their personal information.

55. The Privacy Policy tracks the California statutory definition of "personal information," defining it as "information that you provide to us which personally identifies you, such as your name, email address, or billing information, ***or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account***." *See* Ex. 15 at 28 (emphasis added).

56. The Privacy Policy describes the information it associates with Google Accounts, i.e. "personal information," to include the following:

> The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

See, *e.g.*, *id.* at 2.

57. The document at the "unique identifiers" hyperlink defines a unique identifier as "a string of characters that can be used to uniquely identify a browser, app, or device," which includes cookies, advertising ids and other unique device identifiers. *See*, *e.g.*, *id.* at 29.

58. Google associates these unique identifiers – cookies, IP addresses, User-Agent information, advertising ids, other unique device identifiers, and browsing history information – with individual accounts that include names, email addresses, geolocation, and all other information Google maintains on individual account holders.

59. But Google expressly assures Account Holders that personal information will not be shared with third parties without Account Holders' consent. Specifically, the Privacy Policy makes the following promises:

a. "We do not share your personal information with companies, organizations, or individuals outside of Google except…[1)] "With your consent;" [3)] "With domain administrators;" [3)] "For external processing"; and [4)] "For legal reasons." *E.g.*, Ex. 6 at 6; Ex. 15 at 11-12. Google has made this promise in the Google Privacy Policy since at least March 1, 2012.

b. "We don't share information that personally identifies you with advertisers[.]" *E.g.*, Ex. 12 at 5; Ex. 15 at 5. Google has made this promise in the Google Privacy Policy since at least May 25, 2018.

c. "We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health." *E.g.*, Ex. 12 at 5; Ex. 15 at 5. Google has made this promise in the Google Privacy Policy since at least May 25, 2018.

d. The Google Privacy Policy includes a definition of "sensitive categories" that promises: "We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers [hyperlink] that use our services."[8] *E.g.*, Ex. 12 at 21; Ex. 15 at 22. Google has made this promise in the Google Privacy Policy since at least May 25, 2018.

60. Also, since at least May 25, 2018, Google has acknowledged its responsibility to keep users' personal information secure, stating: "When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information[.]" *E.g.*, Ex. 12 at 1; Ex. 15 at 1; Ex. 20 at 1.

61. Where the Privacy Policy mentions sharing information with "partners," it emphasizes and promises that the information shared is *not* personally identifiable:

> We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

[8] The words "require the same from advertisers" provide a hyperlink to a separate policy titled "Personalized Advertising" detailed below.

E.g., *id.* at 12.

62. But that provision of the Privacy Policy is not protective of personal information. The provision defines "non-personally identifiable information" as "information that is recorded about users so that it no longer reflects or references an individually-identifiable user." *E.g.*, *id.* at 27. That definition conflicts with California law (as set forth above), as well as the definition Google provides elsewhere in the privacy policy, both of which provide that the data Google associates with individual Account Holders is "personal information," regardless of whether it "no longer reflects or references an individual user," and thus does not qualify as "non-personally identifiable information." *See*, *e.g.*, *id.* at 28.

63. Further, Google's statement that it "allow[s] specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies" is limited to the "specific partners" listed in the hyperlink. Those "specific partners" are Nielsen, comScore, Integral Ad Science, DoubleVerify, Oracle Data Cloud, Kantar, and RN SSI Group, and Google promises that their use is limited to "non-personally identifiable information." Ex. 21 at 1. In the section identifying these partners, Google repeats the promise, "We don't share information that personally identifies you with our advertising partners[.]" *Id.* at 2.

4. Google Makes Additional Statements Promising Not to Sell or Share Account Holders' Information

64. In addition to the contractual promises Google makes to Account Holders, Google makes similar promises elsewhere on its website and in the public sphere. These include but are not be limited to: (1) the "Who are Google's Partners" webpage, (2) the Google "Personalized Advertising" webpage, (3) the "We do not sell your personal information to anyone" webpage, (4) the Google "Your privacy is protected by responsible data practices" webpage, (5) Google CEO Sundar Pichai's statement and testimony before Congress when Google was facing inquiry into its privacy practices, and (6) an op-ed from Google CEO Sundar Pichai that was published in the New York Times.

a) The Google "Who are Google's Partners" Webpage Promises

65. As alleged above, the Privacy Policy states that it "allow[s] specific partners [hyperlink] to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies."

66. The hyperlink for "specific partners" takes an Account Holder to the "Who are Google's Partners" webpage where Google reiterates, "***We don't share information that personally identifies you with our advertising partners***, such as your name or email, unless you ask us to share it." Ex. 21 at 2.

67. The same webpage identifies seven "partners" (Nielsen, comScore, Integral Ad Science, DoubleVerify, Oracle Data Cloud, Kantar, and RN SSI Group) that Google permits to "collect or receive ***non-personally identifiable*** information about your browser or device when you use Google sites or apps." *Id.* at 1. Thus, Google promises its account holders that it does not share personal information with those partners.

68. The webpage fails to disclose, however, that Google sends Account Holder personal information to hundreds of other companies ***not*** identified on this page, and that Google works with nearly 1.3 million different publishers that Google sometimes refers to as partners and with which Google routinely shares Account Holder personal information.

b) The Google "Personalized Advertising" Webpage Promises

69. Under the definition of "sensitive categories", the Privacy Policy provides a hyperlink to an Advertising Policies Help webpage titled "Personalized Advertising." *See*, *e.g.*, Ex. 15 at 22.

70. According to Google, the webpage makes promises applicable to "all Google features using personalized advertising functionality." Ex. 22 at 1.

71. On this webpage, Google repeats its promises about sensitive categories, stating:

a. "Advertisers can't use sensitive interest categories to target ads to users or to promote advertisers' products or services." *Id.* at 2.

b. "Personal hardships: Because we don't want ads to exploit the difficulties or struggles of users, we don't allow categories related to personal hardships." *Id.*

c. "Identity and belief: Because we want ads to reflect a user's interests rather than more personal interpretations of their fundamental identity, we don't allow categories related to identity and belief, some of which could also be used to stigmatize an individual." *Id.*

d. "Sexual interests: Because we understand that sexual experiences and interests are inherently private, we don't allow categories related to sexual interests." *Id.*

72. On the same webpage, under the header "Prohibited Categories," Google promises that "[t]he following sensitive interest categories can't be used by advertisers to target ads to users or to promote advertisers' products or services" (*id.*):

a. Restricted drug terms – "Prescription medications and information about prescription medications, unless the medication and any listed ingredients are only intended for animal use and are not prone to human abuse or other misuse." *Id.* at 3.

b. "Personal hardships – We understand that users don't want to see ads that exploit their personal struggles, difficulties, and hardships, so we don't allow personalized advertising based on these hardships. Such personal hardships include health conditions, treatments, procedures, personal failings, struggles, or traumatic personal experiences. You also can't impose negativity on the user." *Id.*

c. "Health in personalized advertising [including] Physical or mental health conditions, including diseases, sexual health, and chronic health conditions, which are health conditions that require long-term care or management[;] products, services, or procedures to treat or manage chronic health conditions, which includes over-the-counter medications and medical devices[;] any health issues associated with intimate body parts or functions, which includes genital, bowel, or urinary health[;] invasive medical procedures, which includes cosmetic surgery[;] Disabilities, even when content is oriented toward the user's primary caretaker. Examples [include] Treatments for chronic health conditions like diabetes or arthritis, treatments for sexually transmitted diseases, counseling services for mental health issues like depression or anxiety, medical devices for sleep apnea like CPAP machines, over-the-counter medications for yeast infections, [and] information about how to support your autistic child." *Id.*

d. "Relationships in personalized advertising [including] Personal hardships with family, friends, or other interpersonal relationships. Examples [include] divorce services, books about coping with divorce, bereavement products or services, family counseling services[.]" *Id.* at 4.

e. "Sexual orientation in personalized advertising [including] lesbian, gay, bisexual, questioning, or heterosexual orientation[.] Examples [include] information about revealing your homosexuality, gay dating, gay travel, information about bisexuality." *Id.* at 4-5.

f. "Personal race or ethnicity." *Id.* at 5.

g. "Personal religious beliefs." *Id.*

c) The Google "We do not sell your personal information to anyone." Webpage Promises

73. On a Google webpage titled "We do not sell your personal information to anyone," Google promises:

a. "We do not sell your personal information to anyone." Ex. 23 at 1.

b. "Without identifying you personally to advertisers or other third parties, we might use data that includes your searches and location, websites and apps that you've used, videos and ads that you've seen, and basic information that you've given us, such as your age range and gender." *Id.*

c. "We give advertisers data about their ads' performance, but we do so without revealing any of your personal information. At every point in the process of showing you ads, we keep your personal information protected and private." *Id.*

d. "[R]emember, we never share any of this personal information with advertisers." *Id.* at 2.

d) The Google "Your Privacy is Protected by Responsible Data Practices" Webpage Promises

74. On its webpage "Your privacy is protected by responsible data practices," Google promises:[9]

a. "Data plays an important role in making the products and services you use every day more helpful. We are committed to treating that data responsibly and protecting your privacy with strict protocols and innovative privacy technologies." Ex. 24 at 1.

b. "We never sell your personal information, and give you controls over who has access[.]" *Id.* at 2.

c. That it uses "advanced privacy technologies [to] help keep your personal information private." *Id.* at 3.

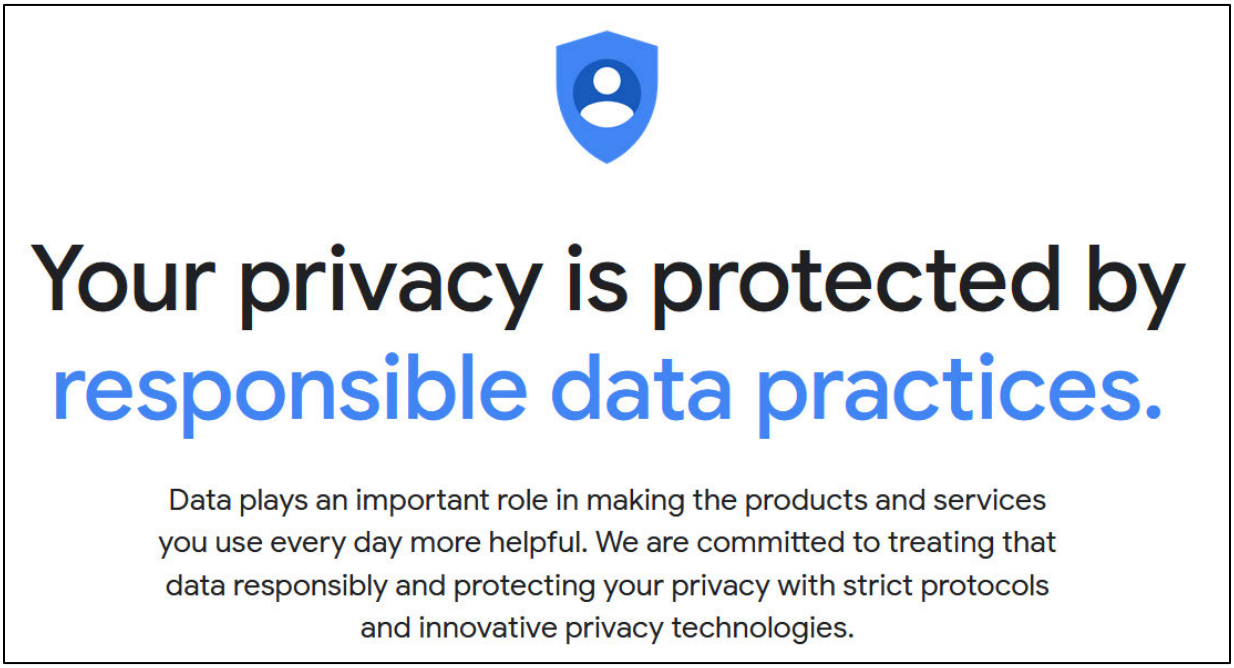
d. "We are continuously innovating new technologies that protect your private information without impacting your experiences on our products." *Id.*

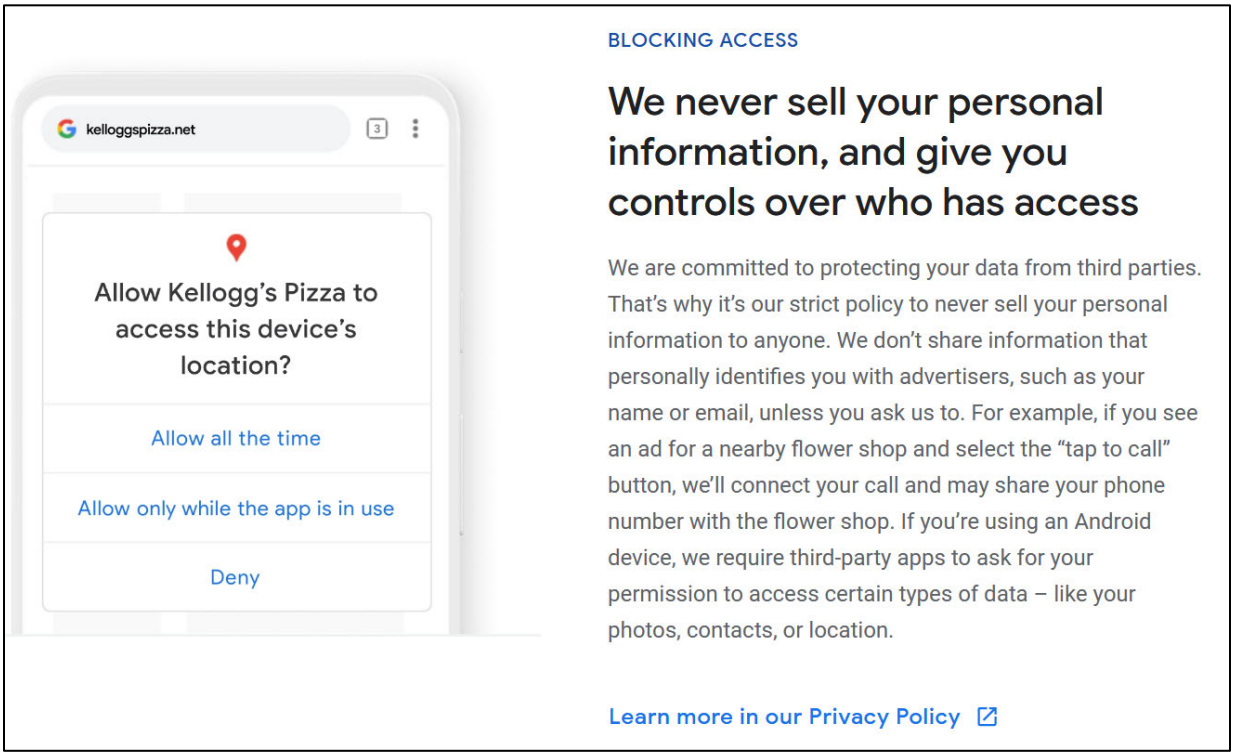
e. "We use leading anonymization techniques to protect your data while making our services work better for you." *Id.* at 3-4.

f. "Privacy is core to how we build our products, with rigorous privacy standards guiding every stage of product development. Each product and feature adheres to these privacy standards, which are implemented through comprehensive privacy reviews." *Id.* at 4.

[9] https://safety.google/intl/en_us/privacy/data/.

75. Screenshot examples from this webpage are provided below:





e) Google CEO Sundar Pichai's Promises

76. On December 11, 2018, Google CEO Sundar Pichai testified on behalf of Google before Congress and repeated the unequivocal promise, "We do not and would never sell consumer data."[10]

77. On May 7, 2019, Google CEO Sundar Pichai published an opinion piece in the New York Times in which he said the following:[11]

> Many words have been written about privacy over the past year, including in these pages. I believe it's one of the most important topics of our time.
>
> People today are rightly concerned about how their information is used and shared, yet they all define privacy in their own ways. I've seen this firsthand as I talk to people in different parts of the world. To the families using the internet through a shared device, privacy might mean privacy from one another. To the small-business owner who wants to start accepting credit card payments, privacy means keeping customer data secure. To the teenager sharing selfies, privacy could mean the ability to delete that data in the future.
>
> Privacy is personal, which makes it even more vital for companies to give people clear, individual choices around how their data is used. Over the past 20 years, billions of people have trusted Google with questions they wouldn't have asked their closest friends: How do you know if you're in love? Why isn't my baby sleeping? What is this weird rash on my arm? We've worked hard to continually earn that trust by providing accurate answers and keeping your questions private. We've stayed focused on the products and features that make privacy a reality — for everyone.
>
> Our mission compels us to take the same approach to privacy. For us, that means privacy cannot be a luxury good offered only to people who can afford to buy premium products and services. Privacy must be equally available to everyone in the world.
>
> * * *
>
> ***To make privacy real, we give you clear, meaningful choices around your data. All while staying true to two unequivocal policies: that Google will never sell any personal information to third parties; and that you get to decide how your information is used.***

[10] *See* Google CEO Sundar Pichai Testifies Before the House Judiciary Committee. December 11, 2018. Available at https://www.c-span.org/video/?455607-1/google-ceo-sundar-pichai-testifies-data-privacy-bias-concerns# (at 1:33:51).

[11] Ex. 25 at 1.

5. A Summary of Google's Promises

78. In sum, Google repeatedly makes the following promises to individuals who sign up for a Google Account:

a. "We don't sell your personal information to anyone." Ex. 5 at 1.

b. "[W]e never sell your personal information to anyone[.]" *Id.*

c. "Advertisers do not pay us for personal information[.]" *Id.*

d. "[W]e never share that information with advertisers, unless you ask us to." *Id.* at 2.

e. "We share reports with our advertisers …, but we do so without revealing any of your personal information." *Id.*

f. "At every point in the process of showing you ads, we keep your personal information protected with industry-leading security technologies." *Id.*

g. "We also never use your … sensitive information like race, religion, or sexual orientation, to personalize ads to you." *Id.* at 1.

h. "We do not and would never sell consumer data." Pichai, *supra* note 10.

i. "We do not share your personal information with companies, organizations, or individuals outside of Google" except in limited circumstances. *See e.g.* Ex. 15 at 11-12.

B. Google Violates its Promises to Account Holders by Selling Their Personal Information on Google RTB

79. Google operates the world's largest ad exchange, the Google Ad Exchange, a digital marketplace that facilitates the buying and selling of advertising inventory. Through the RTB auction process on the Google Ad Exchange, Google shares and sells users' personal information with Google RTB participants to solicit bids for the right to display what is essentially a real-time, near-instantaneous advertisement to a specific user.

80. Thus, the Google RTB is an automated auction system where Google Account Holders' personal information is continually siphoned out and sold to hundreds of participants for advertising purposes.

81. Google RTB bidders bid on the "cost per mille" – the cost per one thousand impressions – which is used to measure how many impressions have been made by an ad.

82. The Google RTB process – from the offer of a targeted ad placement based on a specific user's personal information, to the solicitation of bids, to the sale to the highest bidder, to the placement of the winning bidder's ad on the specific user's personal device – takes less than a hundred milliseconds. For perspective, it takes 300 milliseconds to blink an eye. Hence the name "real time bidding."

83. Google RTB is invisible and undisclosed to Account Holders.

84. To understand the many ways in which Google is selling Account Holders' information, and how many companies Google is selling it to, it helps to first understand the ad ecosystem in which these auctions occur.

85. Account Holders' information passes through multiple layers of what is referred to as an "Ad Stack" as the data is re-directed by Google to various third parties.

86. The Ad Stack consists of between three to five layers depending on the ad:

a. The publisher is the website (or entity controlling the website) that has ad space to sell on its website;

b. The supply side platform ("SSP") is an entity that collects Account Holder data to sell and ad space inventory to populate ads targeted to those account holders;

c. The ad exchange organizes auctions between each side of the ad stack;

d. The demand-side platform ("DSP") bids on behalf of advertisers to show ads to specific account holders; and

e. The advertiser purchases ads targeted to specific account holders.

87. In practice, for any single ad placement to a specific user, the Ad Stack may be compressed. For example, a DSP could place an ad for itself, rather than for another advertiser on whose behalf the DSP has been contracted to submit a bid. If a DSP wins an auction on behalf of itself, the DSP is also the advertiser for that particular ad.

88. Likewise, a publisher in one ad auction may be an advertiser in another. For example, *The New York Times* sells ads targeted to specific users on its own websites through this system – and may also pay for ads targeted to users on other websites.

89. Google compresses the Ad Stack in Google RTB because Google controls significant players at the SSP, ad exchange, and DSP layers of the Ad Stack.

90. On the supply side, Google's AdMob is the most popular SSP for apps on iOS and Android, the two dominant mobile operating systems. AdMob creates software development kits ("SDKs") for publishers to incorporate into their apps. AdMob's SDKs serve as the mechanism for exchanging information between ad exchanges (the auction) and the developers. Within an app, AdMob code collects information and shares it with Google through the bidding process. Google purchased AdMob in 2009. Account Holders' phones share information with Google and ad exchanges.

91. According to the company MightySignal, an analytics firm that "provides detailed and accurate mobile data," Google AdMob is currently installed on:

a. 129,273 apps as of February 1, 2021 – or 82 percent of the Monetization SDK market on Apple devices, including 136 of the top 200 apps in Apple iOS products;[12]

b. 1,013,605 apps as of February 1, 2021 – or 97 percent of the Monetization SDK market on Android devices, included 146 of the top 200 apps on Android.[13]

92. Google's Ad Manager is among the most prominent and used SSP for websites and functions just as AdMob does for smartphone and handheld device apps. Publishers install Google's code on their websites, which make requests to Google tied to identifying cookies.

93. After data leaves an Account Holder's device to be exchanged with the website with which the Account Holder is communicating, Google contemporaneously redirects the Account Holder's personal information and the content of the communication being exchanged with the website to the Google RTB, which, in turn, contemporaneously redirects the personal information and contents to hundreds of different participants on the Google RTB. Google RTB participants then consider the personal information of the Account Holder on whose device the ad will be

[12] https://mightysignal.com/sdk/ios/1162/google-admob

[13] https://mightysignal.com/sdk/android/55931/google-admob

displayed, and calculate how much they are willing to bid for that specific Account Holder (i.e. the Target). As explained above, the entire process takes less time than it does to blink an eye.

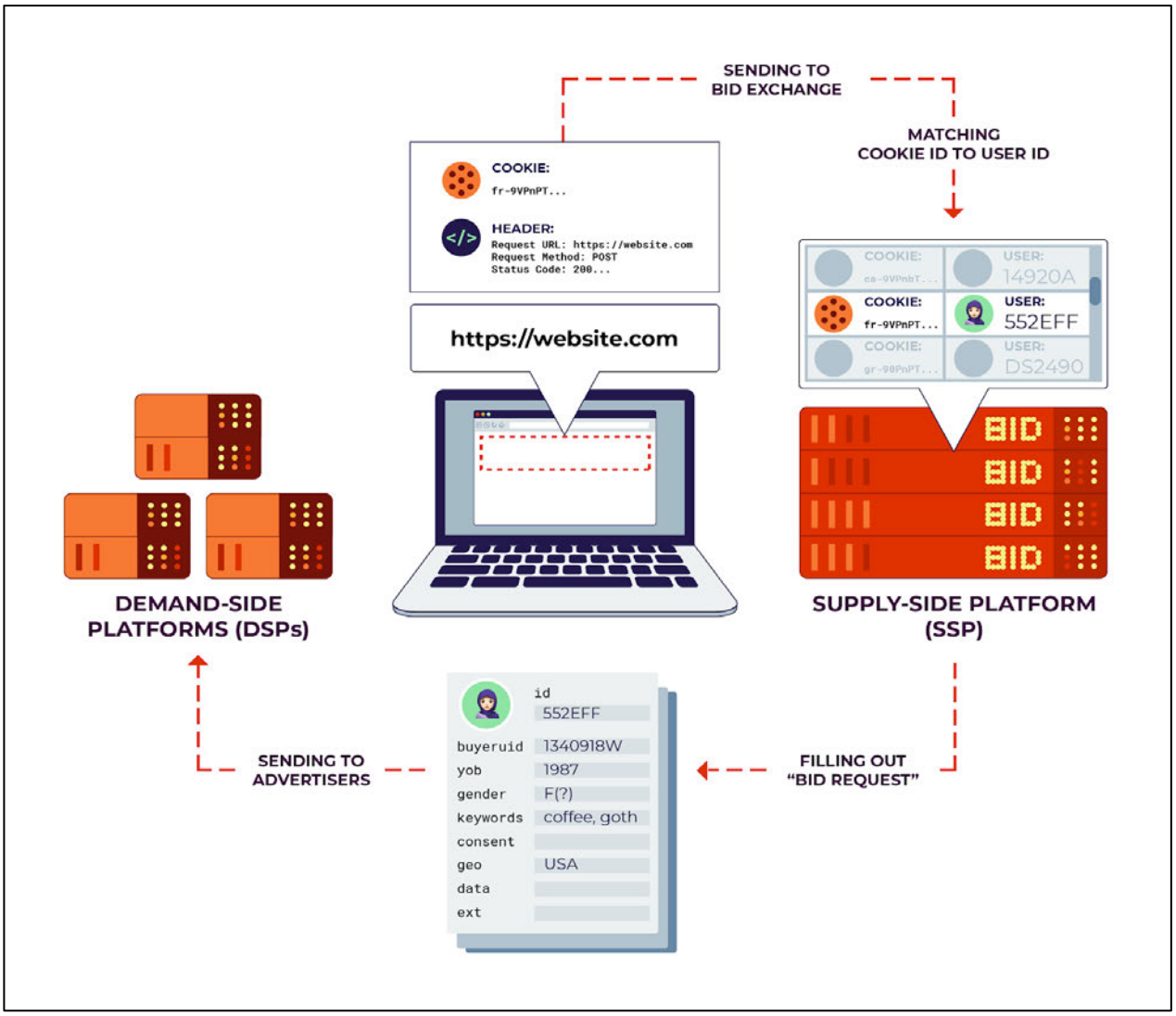
94. The Google RTB sells approximately 53 percent of all ad exchange transactions.

95. On the demand side, Google also has the world's largest DSP. For example, millions of advertisers contract through Google DoubleClick or Google Ads to target specific users with specific attributes.

96. In the Google RTB process, Google sends bid requests to DSPs from publishers to solicit bids from the DSPs based on the personal information of Account Holders. Thus, Google holds the auction and awards the winning bid.

97. All participants in Google RTB are part of the Bidstream, receiving Google's Bid Request, which is the vehicle through which Google sells and shares Account Holder personal information.

98. As illustrated below, the Bid Request moves from the publisher's website (https://website.com in the illustration), to the SSP, to the ad exchange (Google RTB), which fills out a "Bid Request," which is sent to DSPs, who bid on behalf of advertisers based on the personal information that is provided in the Bid Request.



Data flows in a typical real-time bidding system[14]

99. A concrete example helps illustrate the process. Consider a situation where *The New York Times* reserves advertising space on its property to sell through Google RTB. An Account Holder views a specific page, in this example an article on post-partum depression, by entering the web address in the navigation bar of his or her web browser and hits ENTER. This triggers the web browser to send a GET request (or electronic communication) to *The New York Times*, which, in turn, responds by displaying *The New York Times* article on the Account Holder's device. Common

[14] Bennett Cyphers, *Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It.*, Electronic Frontier Foundation (Mar. 19, 2020), https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and.

experience shows that the requested webpage will display in a matter of seconds. But what the Account Holder does not know is that the request to view *The New York Times* article on postpartum depression is also accompanied by a "cookie," which is sent from the Account Holder's web browser to the SSP (recall that an SSP is an entity that collects Account Holder information to sell ad space for targeted advertising). If the SSP is AdMob, which is owned by Google, AdMob matches the cookie to the Account Holder's personal information stored by Google. As one of the preeminent data companies in the world, Google's storage of individuals' personal information is vast and, consequently, its capability to connect cookies to personal information is unprecedented. From Google's vast data store, Google RTB creates a Bid Request – containing the Account Holder's personal information and the content of the specific article that is the subject of the Account Holder's communication. This Bid Request is then sent to DSP participants of the Google RTB (recall that DSPs bid on behalf of advertisers to display targeted ads on available ad space). All Google RTB participants, in turn, can view, collect, and use the information in the Bid Request to determine whether and in what amount they will pay to deliver an ad to the specific Account Holder in question. Bids are submitted and the highest bidder wins the right to place its ad (or its client's ad) on *The New York Times* postpartum depression article that the Account Holder is viewing. This is all done by algorithm and, as set forth above, the entire process takes milliseconds: between the time the Account Holder clicks to access the article and the seconds it takes for the article display, Google RTB has collected, disseminated, and sold the Account Holder's personal information to hundreds of Google RTB participants for the purpose of targeted advertising.

1. The Google RTB Shares Account Holders' Personal Information

100. Google publishes several documents in which it explains how Google RTB Bid Requests are structured. Among them are documents titled:

a. OpenRTB Integration;[15]

[15] https://developers.google.com/authorized-buyers/rtb/openrtb-guide

b. Real-Time Bidding Protocol Buffer v.199;[16]

c. Authorized Buyers Real-time Bidding Proto;[17] and

d. Infrastructure Options for RTB Bidders (part 4).[18]

a) OpenRTB Integration

101. OpenRTB Integration provides a chart with "Bid request variables and definitions" involved in Google OpenRTB.

102. The following chart provides a subset of the Bid Request variables that OpenRTB Integration shares with developers:

CATEGORIES	
site	Details about the publisher's website.
app	Details about the publisher's app.
device	Details about the user's device to which the impression will be delivered.
user	Details about the human user of the device; the advertising audience.
name	Site or app name.
domain	Domain of the site or app. For example, "foo.com".
COMMUNICATIONS CONTENT	
cat	Array of IAB content categories of the site or app.
sectioncat	Array of IAB content categories that describe current section of site or app.
pagecat	Array of IAB content categories that describe current site or app page or view.
page	URL of the page where the impression will be shown.
ref	Referrer URL that caused navigation to the current page.
publisher	Details about the Publisher object of the site or app.
content	Details about the Content within the site or app.
keywords	Comma-separated list of keywords about this site or app.
content id	ID uniquely identifying the content.
episode	Content episode number (typically applies to video content).
title	Content title. Video examples: "Search Committee" (television); "A New Hope (movie); or "Endgame" (made for web). Non-video example: "Why an Antarctic Glacier is Melting So Quickly" (Time magazine article).
series	Content series. Video examples: "The Office" (television); "Star Wars" (movie); or "Arby 'N' The Chief (made for web). Non-video example: ("Ecocentric") (Time magazine blog).
DEVICE	
dnt	Standard 'Do Not Track' flag as set in the header by the browser.
ua	Browser user-agent string.
ip	IPv4 address closest to device.
geo	Location of the device assumed to be the user's current location defined by a Geo object.
didsha1	Hardwire device ID.

[16] https://developers.google.com/authorized-buyers/rtb/downloads/realtime-bidding-proto

[17] https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide

[18] https://cloud.google.com/solutions/infrastructure-options-for-rtb-bidders

dpidsha1	Platform device ID (e.g. Android ID).
ipv6	IPv6 address closest to device.
carrier	Carrier or ISP, using exchange curated string names which should be published to bidders a priori.
make	Device make (e.g. Apple).
model	Device model (e.g. iPhone).
os	Device operating system (e.g. iOS).
osv	Device operating system version.
hwv	Hardware version of the device (e.g. '5S' for iPhone 5S).
devicetype	The general type of device.
ifa	ID sanctioned for advertiser use in the clear.
macsha1	MAC address of the device.
GEO-LOCATION	
lat	Latitude from -90.0 to 90.0, where negative is south.
lon	Longitude from -180.0 to 180.0 where negative is west.
country	Country.
region	Region.
metro	Google metro code; similar to but not exactly Nielson DMAs.
city	City using United Nations Code for Trade & Transport.
zip	Zip/postal code.
type	Source of location data.
accuracy	Estimated location accuracy.
lastfix	Number of seconds since this geolocation fix was established.
USER	
Id	Exchange-specific id for the user.
Buyerid	Buyer-specific ID as mapped by the exchange for the buyer.
Gender	Gender as 'M' male, 'F' female, 'O' other.
Keywords	Comma-separated list of keywords, interests, or intent.
Customdata	Optional feature to pass bidder data set in the exchange's cookie.
Geo	Location of the user's home based defined by a Geo object. This is not necessarily their current location.
Data	Values for this field are now redacted. Segment.id references the exchange-detected vertical of the page. Segment.value corresponds to the weight of that detected vertical, a higher weight suggesting the page is more relevant for the detected vertical.

b) Real-Time Bidding Protocol Buffer v.199

103. Real-Time Bidding Protocol Buffer v.199 provides further details. It explains of the protocol buffer, "This is the message that Google uses to request bids" and confirms that the same categories of personal information are sent to bidders as those set forth in the OpenRTB Integration chart (see above).

104. Real-Time Bidding Protocol Buffer v.199 illustrates that the personal information about an Account Holder is the key item for sale based on the order in which the re-directed data is provided from Google to the bidders.

105. As shown in Real-Time Bidding Protocol Buffer v.199, data is shared in the following order:

SPECIFIC REQUEST IDENTIFIER		
1	BidRequest	Unique request id generated by Google. This is 16 bytes long.
"INFORMATION THAT WE KNOW ABOUT THE USER"		
2	IP address	The first 3 bytes of IPv4 or first 6 bytes for IPv6.
3	Special Treatment	Reasons for special treatment of user data. For example, if the "current request should be treated as child-directed for purposes of the Children's Online Privacy Protection Act."
4	Google ID	"The Google ID for the user. … This field may be the same as the Google ID returned by the cookie matching service."
5	Google ID Version	"The version number of the google_user_id. We may sometimes change the mapping from cookie to google user id."
6	Google ID Age	"The time in seconds since the google user id was created."
7	Match Data	"Match data stored for this google_user_id through the cookie matching service. If a match exists, then this field holds the decoded data that was passed in the google hm parameter."
8	User-Agent	"A string that identifies the browser and type of device that sent the request."
9	FLoC	"The value of a cohort ID – a string identifier that is common to a large cohort of users with similar browsing habits. … Experimental feature: may be subject to change."
10	User Agent Information	"This will be populated with information about the user agent, extracted from the User-Agent header."
11	Publisher location	The billing address country of the publisher.
12	End-user location	The user's approximate geographic location.
13	Zip code	Detected postal code of the user.
14	Hyperlocal	A hyperlocal targeting location when available.
15	User verticals	"List of detected user verticals. Currently unused. This field is not populated by default. We recommend that bidders instead store and look up list ids using either google_user_id or hosted-match-data as keys."
16	User-list	The user list id.
"INFORMATION THAT WE KNOW ABOUT THE WEB PAGE OR MOBILE APP"		
17	Publisher ID	The publisher ID.
18	Seller network ID	The seller network ID.
19	Partner ID	ID for the partner that provides this inventory.
20	URL	The URL of the page with parameters removed.
21	Bool	Indicates that the request is using semi-transparent branding which means only a truncated version of the request URL provided.
22	String	An id for the domain of the page that is set when the inventory is anonymous.
23	String language	Detected user languages based on the language of the webpage.
24	Detected Verticals	One or more detected verticals for page as determined by Google.
25	Vertical Weight	Weight for each vertical.
26	Ordered Verticals	Orders list of detected content verticals.
27	Content Labels	List of detected content labels.

AUCTION INFORMATION		
28	Unique ID	A unique ID for the overall query.
29	Auction type	The type of auction that will be run for this query.
"INFORMATION ABOUT THE DEVICE"		
30	Type	Phone, tablet, desktop, connected TV, game console, or set-top box.
31	Platform	Examples: Android, iPhone, Palm.
32	Brand	Examples: Nokia, Samsung.
33	Model	Examples: N70, Galaxy.
34	Operating System	Contains the OS version for the platform.
35	Mobile Carrier	Unique identifier for the mobile carrier.
36	Screen-width	As measured in pixels.
37	Screen-height	As measured in pixels.
38	Screen pixel ration millis	Screen Density
39	Orientation	Portrait or Landscape
INFORMATION FOR "AD QUERIES COMING FROM MOBILE DEVICES"		
40	Mobile	If true, then this request is coming from a smartphone or tablet.
41	Mobile App	The identifier of the mobile app or mobile webpage. "If the app was downloaded from the Apple iTunes app store, then this is the app-store id, e.g. 343200656. For Android devices, this is the fully qualified package name, e.g. com.rovio.angrybirds. For Windows devices, it's the App ID, e.g. f15abcde-f6gh-47i0-j3k8-37193817mn3o. For SDK-less requests (mostly from connected TVs), the app ID provided by the publisher directly in the request."
42	Interstitial	If true, then this is a mobile full screen ad request.
43	App Category	The IDs of categories to which the current mobile app belongs.
44	Mobile Optimized	This indicates whether the page is optimized for mobile browsers on high-end phones.
45	Advertising IDs	This field is used for advertising identifiers for: 1) iOS devices (This is called Identifier for Advertising or IDFA, as described at https://support.google.com/authorizedbuyers/answer/3221407); 2) Android devices; 3) Roku devices; 4) Microsoft Xbox devices; 5) Amazon devices (i.e. Amazon Fire)
46	App Name	App names for Android by Google Play and for iOS by App Annie.
47	App User Rating	Average User rating for the app.
48	Bidder SDK	Identification of and information about an SDK installed in the publisher's app that the bidder has access to, often because it's the bidder's SDK.
49	SKAdNetwork	Publisher's SKAdNetwork information to support app installation attribution for iOS 14 and later.
VIDEO INFORMATION		
50	Placement	Where the ad is placed.
51	URL	The URL of the page that the publisher gives Google to describe the video content, with parameters removed.
52	Playback Method	How the video ad will be played.
53	Clickable	Describes whether the video ad is clickable.
54	Start-Delay	The time in milliseconds from the start of the video when the ad will be displayed.
55	Ad Duration	The minimum and maximum ad durations.

56	Skippable	Whether the publisher allows users to skip the ad.
57	Protocols	Supported video protocols.
58	File formats	Supported video file formats.
59	Companion Ads	Information about companion ad slots shown with the video.
60	Size	Height and width for the video ad.
61	Video title	The video title.
62	Video keywords	A list of keywords describing the video, extracted from the content management system of the video publisher.

106. The above chart indicates that "User verticals" are among the types of information that have been sold to and shared with Google RTB participants. Verticals pertain to a marketing technique known as "vertical segmentation," and is used to facilitate targeted advertising by identifying users as falling within particular categories, segments, and subcategories. Segments include health, religion, ethnicity, nationality, and sexuality. These categories of information therefore reflect the information that Google knows about each Account Holder's personal characteristics.

107. Google's acknowledged use, disclosure, and sale of a "list of detected user verticals" therefore constitutes a substantial invasion of Account Holders' privacy.

108. Some of the categories used by Google are made available on its developer pages.[19] For example:

a. The People & Society segment includes the following verticals: LGBT, Men's Interests (mature), and Divorce & Separation.

b. The Ethnic & Identity Groups segment includes the following verticals: Africans & Diaspora, African-Americans, Arabs & Middle Easterners, Asians & Diaspora, East Asians & Diaspora, Southeast Asians & Diaspora, Eastern Europeans, Indigenous Peoples, Native Americans, Jewish Culture, Latinos and Latin-Americans, and Western Europeans.

c. The Religion & Belief segment includes the following verticals: Buddhism, Christianity, Hinduism, Islam, Judaism, Scientology, Skeptics & Non-Believers, and Spirituality.

[19] https://developers.google.com/adwords/api/docs/appendix/verticals

d. The Health segment includes the following verticals:

HEALTH VERTICALS CATEGORIES			
Acne & Blem. Treatments	Weight Loss	Aging & Geriatrics	Alzheimer's Disease
Cleansing and Detox.	Steroids & PEDs	AIDS & HIV	Allergies
Arthritis	Blood Sugar & Diabetes	Cancer	Ear Nose & Throat
Eating Disorders	Endocrine Conditions	Thyroid Conditions	GERD & Diges. Disorders
Genetic Disorders	Heart & Hypertension	Cholesterol Issues	Infectious Diseases
Parasites & Parasitic Dis.	Vaccines & Immunizations	Injury	Neurological Conditions
Learn. & Dev. Disabilities	ADD & ADHD	Obesity	Pain Management
Headaches & Migraines	Respiratory Conditions	Asthma	Skin Conditions
Sleep Disorders	Doctor's Offices	Hospitals & Treat. Centers	Surgery
Cosmetic Surgery	Physical Therapy	Men's Health	Mental Health
Anxiety & Stress	Counseling Services	Depression	Toxic Sub. & Poisoning
Reproductive Health	Birth Control	Infertility	Male Impotence
OBGYN	Sex Ed. & Counseling	Sexual Enhancement	STDs
Substance Abuse	Drug & Alcohol Testing	Drug & Alc. Treatment	Smoking & Sm. Cessation

109. Each of these verticals comprise personal information under California law and Google's policies.

c) Authorized Buyers Real-time Bidding Proto

110. Until sometime in February or March 2021, Google's developer tools included "sample bid requests and response," which illustrate how Account Holders' information in verticals are shared and sold through Bid Requests, on a developer page called Authorized Buyers Real-time Bidding Proto. The sample Bid Request for an app banner provides that the following data would be included among the bidstream sent from Google to the authorized bidder:

```
user {
  id: "7T0uAql92ru9Ndd90Pnh73lsY2L"
  data {
    id: "DetectedVerticals"
    name: "DoubleClick"
    segment {
      id: "236"
      value: "0.2"
    }
    segment {
      id: "457"
      value: "0.2"
    }
```

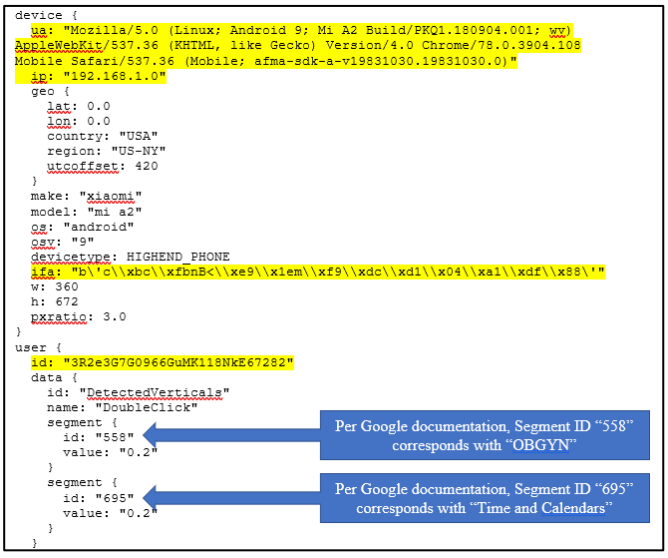
This code tells the bidder that the Account Holder with the id 7T0uAq192ru9Ndd90Pnh73lsY2L is in the "weight loss" (236) and "special and restricted diets" (457) segments.[20]

[20] The complete list of verticals, including both the descriptor (e.g., Weight Loss) and corresponding segment ID (e.g., 236), is available at: https://developers.google.com/adwords/api/docs/appendix/verticals.

111. Another example provided by Google showed an Account Holder with the ID iE0B3ASr55t81Mf8XnJ34W084h8 is in the "Pregnancy and Maternity" vertical:

See Exhibit 27.

112. Another exemplar identifies the Account Holder with id 2R2e3G7G096GuMK118NkE67282 is in the vertical "OBGYN":



See Exhibit 28.

113. Sometime in February or March 2021, Google removed these exemplars that show the line of code specifying "DetectedVerticals" for Account Holders. On March 14 or 15, 2021, Google also replaced what had previously been labeled as Real-Time Bidding Protocol Buffer

v.198 with v.199 (the latter referenced above in this Complaint). As set forth above, Real-Time Bidding Protocol Buffer v.199 now claims that "User verticals" are unused. *See supra* at ¶ 105, Row 15. This is a distinction without a difference because Real-Time Bidding Protocol Buffer v.199 specifies that Google *does* include "Detected Verticals" for each page or app where the Google RTB auction sales system is in place. *See supra* at ¶ 105, Row 24.

114. Google's statement that "user verticals" are "unused" may simply reflect the fact that the inferred information contained in those verticals has been transferred to the new FLoC value, which Google describes in the Real-Time Bidding Protocol Buffer v.199 as "[t]he value of a cohort ID – a string identifier that is common to a large cohort of users with similar browsing habits." As the Electronic Frontier Foundation detailed in a recent article, "[i]t is highly likely that FLoC will group users" by gender, ethnicity, age, income, mental health and "may also directly reflect visits to websites related to substance abuse, financial hardship, or support for survivors of trauma."[21]

115. Moreover, the "Detected Verticals" still constitute "personal information" under California law because they are inferred data about web-browsing history that Google is selling and from which Google RTB participants can compile and augment their own detailed dossiers about Account Holders. Google still sells and shares these verticals and segments with approved bidders in Google RTB together with Account Holders' Google ID and other identifiers.

[21] Bennett Cyphers, *Google's FLoC Is a Terrible Idea*, Electronic Frontier Foundation (Mar. 3, 2021), https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea.

d) Infrastructure Options for RTB Bidders (Part 4)

116. In the article "Infrastructure Options for RTB Bidders (Part 4)" ("Infrastructure Options"), Google notes that a Google RTB bidder may do the following:

Bidding

A bidder performs the following tasks:

- **User matching**: Identify the (unique) user.
- **Selecting segments**: Retrieve and select the (unique) user's segments and their price.
- **Deciding whether to bid**: Some bids are too expensive, and some ad requests might not match any existing campaigns. A bidder should be able to refuse a bid. This refusal saves processing time and resources.
- **Selecting relevant ads**:** **If the bidder decides to bid then the bidder must also select an ad. Selecting the right ad can improve the odds that a user might click and possibly generate a conversion.
- **Optimizing bids**: A bidder should always try to find the minimum bid price that will still win the auction.
- **Building a bid response**: Using OpenRTB or a custom application, build and return a bid response serialized in protobuf or JSON format. The response should include information such as the ad URL, the bid, and the win URL endpoint that can be called if the bid wins.

117. For "user matching," the article encourages Google RTB participants to collaborate on creating "match tables" that would enable them to sync cookies and identify users across multiple platforms. The article further directs the reader to a hyperlink to learn more about "[h]ow cookie matching works in real-time bidding." As explained below, cookie matching is a Google service that enables Google RTB participants to match cookie identifiers to participants' existing individual profiles.

118. For "selecting segments," Google explains that the Google RTB system can "extract user segments from the (unique) user profile store [hyperlinked], order the segments by price, and filter for the most appropriate segment."

119. The link to "(unique) user profile store," explains that "[t]his store contains (unique) users and their associated information that provide key insights to select a campaign or ad on request. Information can include the (unique) user's attributes your own segments, or segments

imported from third-parties. In RTB, imported segments often include bid price recommendations."[22]

120. The "(unique) user profile store" goes on to explain: "The store is updated frequently based on the (unique) user's interaction with ads, sites they visit, or actions they take. The more information, the better the targeting. You might also want to use third-party data management platforms (DMPs) to enrich your first-party data."

121. Thus, Google's internal documents indicate that in addition to sharing Account Holders' personal information in the Google RTB Bidstream, Google is also grouping Account Holders into targeted advertising segments, which includes sensitive categories related to race, religion and sexual orientation, compiling in-depth personal profiles, and then using those profiles in furtherance of the Google RTB.

122. Independent research has confirmed that Google allows targeted advertising based on sensitive categories. In a 2015 study, researchers created an automated tool called AdFisher to "explore[] how user behaviors, Google's ads, and Ad Settings interact." The researchers started with a group of 500 fresh simulated browser instances. They then sent part of the group to the top 100 websites for substance abuse as listed on Alexa while the remainder acted as a control group and did nothing. Next, the researchers sent both browser groups the Times of India, a content-providing webpage that uses Google for advertising. The ads displayed on the Times of India for both groups were collected and analyzed, to determine whether there was any difference in the outputs shown to the agents. For the substance abuse group, the top three ads shown to them were for an alcohol and drug rehabilitation center called the Watershed Rehab, with these top three ads making an appearance, respectively, 2,276 times, 362 times, and 771 times. The non-substance-abuse group was not shown the Watershed Rehab ads a single time.[23]

---

[22] https://cloud.google.com/solutions/infrastructure-options-for-serving-advertising-workloads#unique_user_profile_store

[23] Amit Datta, Michael Carl Tschantz, and Anupam Datta, Automated Experiments on Ad Privacy Settings, Proceedings on Privacy Enhancing Technologies 2015; 2015 (1):92-112, available at https://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf. Despite this, the browsers visiting substance abuse websites showed no impact on the "Ad Settings" page that Google makes available to Account Holders for the purported purpose of letting those Account Holders understand inferred

123. Account Holders have no idea that they have been associated with these categories, and no way to prevent being targeted by their association with them. Indeed, the same article reported that despite the obvious, statistically significant return of drug rehabilitation ads for the substance abuse group when compared non-substance abuse group, the Ad Settings page for members of each group were not different. "Thus," the researchers concluded, "information about visits to these websites" – the 100 websites for substance abuse – "is indeed being used to serve ads, but the Ad Settings page does not reflect this use in this case. Rather than providing transparency, in this instance, the ad settings were *opaque* as to the impact of this factor." (emphasis in original).

124. The above study is not an outlier. A 2019 study confirms that data collection and behavioral tracking information is aggregated to derive user interest profiles, which in turn are leveraged by advertising platforms, like Google RTB, to (1) expand their own data profiles on individual users, and (2) to sell more expensive ads that are more specifically targeted. Significantly, the 2019 study noted that Google has unprecedented visibility into users' browsing behavior because it is able to collect and aggregate user information from a vast array of sources, either owned by Google or accessible to Google by virtue of Google's embedded source code.[24] Google can therefore infer user interests to an alarmingly accurate degree.[25]

125. In 2012, researchers at Worchester Polytechnic Institute conducted a focused study of the Google ad network. The study found, among other things, that non-contextual ads were shown related to induced sensitive topics regarding sexual orientation, health, and financial matters. By way of background, contextual ads are those that derive from the content of the webpage that a

---

interests that Google has assigned. The study also showed that browser instances identified as women were 6 times less likely to be shown ads for high-paid executive positions than similarly-situated male browser instances.

[24] Muhammad Ahmad Bashir, et al., Quantity vs Quality: Evaluating User Interest Profiles Using Ad Preference Managers, Network and Distributed Systems Security (NDSS) Symposium 2019 (February 24-27, 2019), available at https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_04B-5_Bashir_paper.pdf.

[25] Only platforms that can observe users on a given site (i.e. by being directly embedded in the site, or by partnering with another third-party that is embedded[]) can draw such an inference. *Id.*

user is viewing, e.g. shoe ads being displayed on a website selling shoes. Conversely, non-contextual ads have no relation to the webpage content, e.g. ads for mental health treatment on a website selling shoes. Thus, the fact that the 2012 study found that the Google ad network was able to facilitate non-contextual ads related to induced sensitive categories supports the conclusion that sensitive information is being sold by the Google ad network to foster targeted advertising.[26]

126. Account Holder information sold and shared by Google with advertising bidders constitutes personal information as defined by both Google and California law. The information shared by Google through its RTB process is personal information that is reasonably capable of being associated, or that could reasonably be linked, directly or indirectly, with a particular consumer or household. Cal. Civ. Code § 1798.140(o)(1). In fact, it is not only "capable" of being associated but *is being* associated with a particular consumer. That is, after all, the entire purpose of Google RTB.

127. The above studies and examples demonstrate that Google violates its express privacy promises not to share Account Holders' personal information each time it shares and sells their information, including information contained in verticals and segments, with participants in Google's RTB process. Moreover, each time Google shares information in segments concerning health, religion, ethnicity, race, or sexuality, Google violates its express promises to Account Holders that it will never share or sell their sensitive personal information.

2. The Data Google Discloses is Designed to be Personally Identifiable to Google RTB Participants

128. Google is not sharing anonymized, non-personally identifiable data to just a few "partners," as Google suggests in one paragraph in its Terms of Service. To the contrary, the data it sells and shares with participants on the Google RTB is tied to unique identifiers that track specific Account Holders across web and physical activity, including where they are, what they are doing, and what they purchase, and draw inferences from that data of the sort derived from and

[26] Craig E. Wills and Can Tartar, Understanding What They Do with What They Know (Short Paper), *WPES'12*, October 15, 2012, available at: https://web.cs.wpi.edu/~cew/papers/wpes12.pdf.

constituting the kinds of sensitive verticals described above. All of this data is tied to unique persistent identifiers.

129. Critically, the data Google sells allows its RTB participants not only to target Account Holders specifically, but also to build from scratch or cross-reference and add to the data that they already have in ***their*** own detailed profiles for Account Holders.

130. For example, Facebook is a frequent bidder in Google RTB and, in addition to the personal information received from Google, Facebook has its own database of account holder names, email addresses, phone numbers, device IDs, likes, interests, and friends.[27] A large data company like Facebook is therefore able to connect the personal information made available by Google RTB to its own existing databases, matching certain of the information in the Account Holder's profile, such as the IP address, to information already in Facebook's possession.

131. The consequence is two-fold.

132. ***First***, Google provides Facebook with personal information that Facebook uses to specifically identify the account holder for the purpose of bidding on an ad in Google's Ad Exchange. Recent reports in *The Wall Street Journal* and *The New York Times* indicate that, in exchange for Google helping Facebook to recognize specific mobile and web users, Facebook agreed to place bids through Google RTB for 90 percent of the users it recognizes and to spend at least $500 million per year on the Google Ad Exchange.[28] Put differently, Google helped Facebook deanonymize its account holders in exchange for at least one half billion dollars.

133. Neither Google nor Facebook denied the existence of the deal or its terms in response to these reports. To the contrary, Google's response hinted that its deal with Facebook was not unique, stating that it is just "one of over 25 partners participating in Open Bidding" inside

[27] *See* www.facebook.com/privacy.

[28] Daisuke Wakabayashi and Tiffany Hsu, *Behind a Secret Deal Between Google and Facebook*, The New York Times (Jan. 17, 2021), available at https://www.nytimes.com/2021/01/17/technology/google-facebook-ad-deal-antitrust.html; Ryan Tracy and Jeff Horwitz, Inside the Google-Facebook Ad Deal at the Heart of a Price-Fixing Lawsuit, The Wall Street Journal (Dec. 29, 2020), available at https://www.wsj.com/articles/inside-the-google-facebook-ad-deal-at-the-heart-of-a-price-fixing-lawsuit-11609254758.

the Google Ad Exchange.[29] This significant admission supports the conclusion that Google is selling Account Holders' personal information – presumably to the highest bidder, or perhaps to itself when it sees fit.

134. ***Second***, whether or not Facebook (or another DSP or advertiser) submits a winning bid, participating in the auction facilitates the acquisition and retention of Account Holders' personal information that Google RTB participants can and do use to create or continuously update and augment their own existing user data troves.

135. This is true even for Google RTB participants who are not as large as Facebook and who do not have their own consumer account holders. Google actively assists Google RTB participants in matching Account Holder information made available in a Bid Request to the information those participants already have about specific individuals through a "cookie matching service."

136. According to Google, "[c]ookie matching is a feature that enables" Google RTB participants "to match [their own cookie] – for example, an ID for a user that browsed your website – with a corresponding bidder-specific Google User ID, and construct user lists that can help you make more effective bidding choices."[30] Specifically:

> In the context of digital advertising, Google identifies users with cookies that belong to the `doubleclick.net` domain, and bidders participating in Real-Time Bidding may have their own domain where they identify some set of users they would like to show ads. Cookie Matching enables the bidder to match their cookies with Google's, such that they can determine whether an impression sent in a bid request is associated with one of users being targeted, they will receive either their own cookie data or a bidder-specific Google User ID that is an encrypted form of the `doubleclick.net` cookie in the bid request.
>
> The cookie matching service described in this guide facilitates the creation and maintenance of the association between a bidder's cookie and the Google User ID, and also allows one to populate user lists.

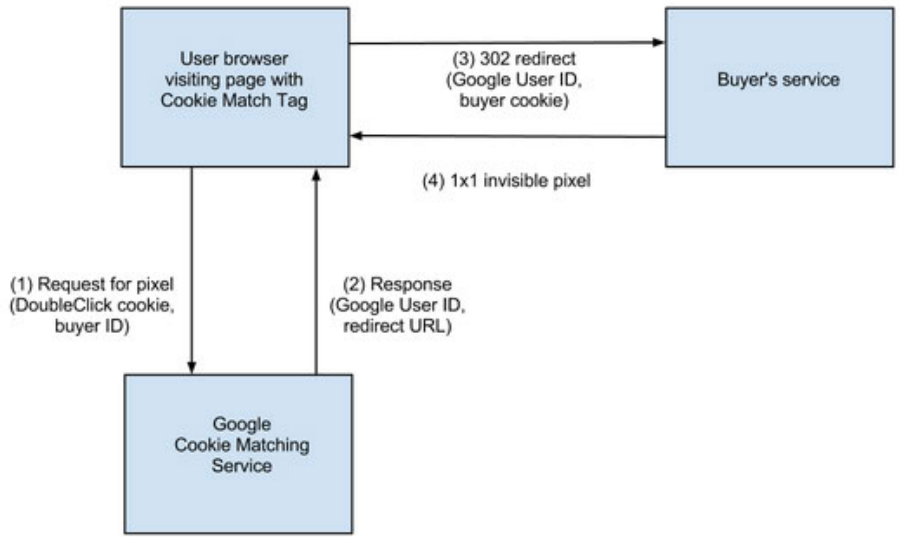
137. Google illustrates how cookie matching works:

[29] Adam Cohen, *AG Paxton's misleading attack on our ad tech business* (Jan. 17, 2021), https://blog.google/outreach-initiatives/public-policy/ag-paxtons-misleading-attack-on-our-ad-tech-business/.

[30] Cookie Matching, https://developers.google.com/authorized-buyers/rtb/cookie-guide.

Cookie Matching workflow diagram

This workflow is illustrated by the diagram below, where requests and responses are represented by an arrow, and the data items that accompany them are listed in parentheses.



138. Thus, Google RTB participants are able to match the alphanumeric id of the Google ID shared in the Bid Request with the auction participants' (including Surveillance Participants') own unique cookie identifier for the Account Holder. In other words, even though the Google ID is purportedly anonymous, Google provides participants a key, via cookie matching, to determine exactly who certain Account Holders are. If the Account Holder whose profile is up for bid also has an account id with the participant, cookie matching will not only let the participant know that fact, it will enable the participant to tie the personal information from Google RTB together with data it already has to enhance its profile of the Account Holder.

139. In an indication that Google realizes its cookie matching process violates California law, the Cookie Matching page states a "Key Point" that "the Google User ID will not be specified in the bid request" for "users detected to originate from California," but the bidder will "still receive … hosted match data" to inform bidding.[31]

[31] *Id.*

> **Key Point:** For users detected to originate from California, the Google User ID will not be specified in the bid request. You will still receive your hosted match data, which can be used to inform your bidding logic.

140. But this "Key Point" cannot absolve Google. It does not change the fact that Google is disclosing personal information about the Account Holder directly to the "buyer's service." By still providing the "buyer's service" with the "hosted match data," Google is connecting its own Google User ID to the buyer's user id, which is also personal information.

141. Cookie matching permits Google to share and sell Account Holders' personal information with participants ***even when Account Holders take steps to avoid Google's tracking***. By constructing "user lists," which include Account Holders, Google RTB auction participants can reidentify people even when different identifiers are used, purportedly to prevent that kind of targeting.

142. As Google explains to its developers: "Cookie Matching enables the bidder to match their cookies with Google's, such that they can determine whether an impression sent in a bid request is associated with one of users being targeted."[32] And Google explains to developers that the purpose of this is to allow third parties to associate information with Account Holders: "The cookie matching service described in this guide facilitates the creation and maintenance of the association between a bidder's cookie and the Google User ID, and ***also allows one to populate user lists***" (emphasis added).[33]

143. Notably, Google ***encourages*** Google RTB participants to "store" these user lists, inviting them to retain keys to defeat de-identification processes: "We recommend that bidders instead store and look up list ids using either google_user_id or hosted_match_data as keys."[34] That is, ***rather than protecting Account Holders' privacy, Google encourages its partners to invade it.***

---

[32] *Id.*

[33] *Id.*

[34] Real-Time Bidding Protocol Buffer v.202, https://developers.google.com/authorized-buyers/rtb/downloads/realtime-bidding-proto

144. The Google Cookie Matching service is ubiquitous. A 2019 analysis by the web browser Brave showed that a single hour of web browsing resulted in 318 different Google cookie matches with at least 10 different companies participating in RTB auctions.[35]

145. Through Google Cookie Matching and through Google's ubiquitous presence on the Internet, participants in Google RTB are sold and provided with personal information through which they can and do build rich user dossiers based on the vast majority of every Internet Account Holder's browsing history.

146. A 2018 study co-authored by Professor Wilson found that 52 different companies "observe at least 91 percent of an average user's browsing history under reasonable assumptions about information sharing within RTB auctions" and 636 companies "observe at least 50 percent of an average user's impressions."[36]

147. Further, a recent investigation by *The New York Times* reveals how easy it is to tie what Google and others characterize as anonymous pieces of data together to identify a specific person. In an article titled "They Stormed the Capitol. Their Apps Tracked Them," writers Charlie Warzel and Stuart Thompson explain how they were able to identify specific individuals who participated in the attack on the United States Capitol on January 6, 2021 through a database of purportedly "anonymous" information that was provided to them by an industry insider.[37]

148. The article illustrates how an Account Holder's precise movements could be tracked across the country using purportedly anonymous data. For example, one person shown to have been near the Capitol during the attack was Ronnie Vincent from Kentucky. Starting with what the industry deemed anonymous data, *The New York Times* identified Vincent and tracked his specific path to and within Washington D.C.:

---

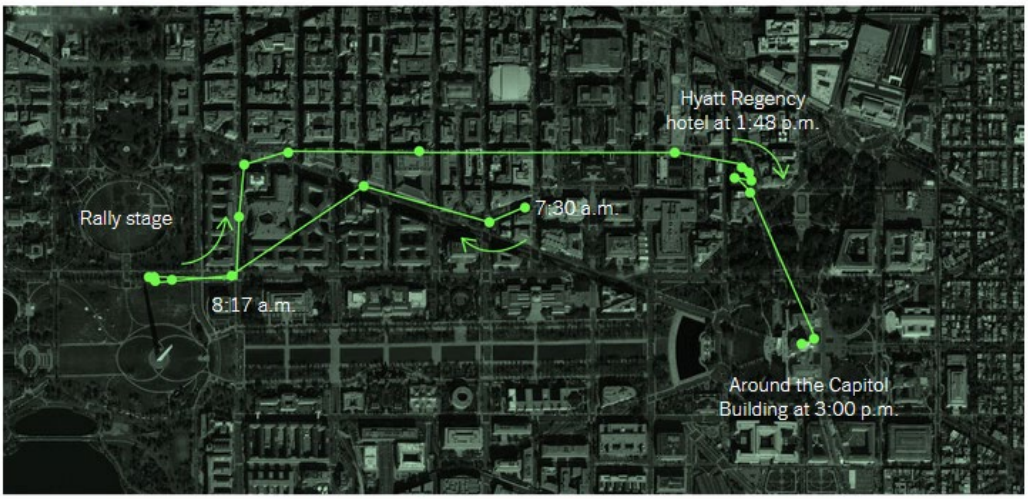
[35] Dr. Johnny Ryan, RTB Header Bidder Evidence – Explanatory Document, Brave, Inc. (Sept. 2, 2019), https://brave.com/wp-content/uploads/explanatory_note_google_RTB_and_push_pages.pdf

[36] Muhammad Ahmad Bashir and Christo Wilson, "Diffusion of User Tracking Data in the Online Advertising System," Proceedings on Privacy Enhancing Technologies 2018 (4):85-103, at 86, https://www.ccs.neu.edu/home/ahmad/publications/bashir-pets18.pdf.

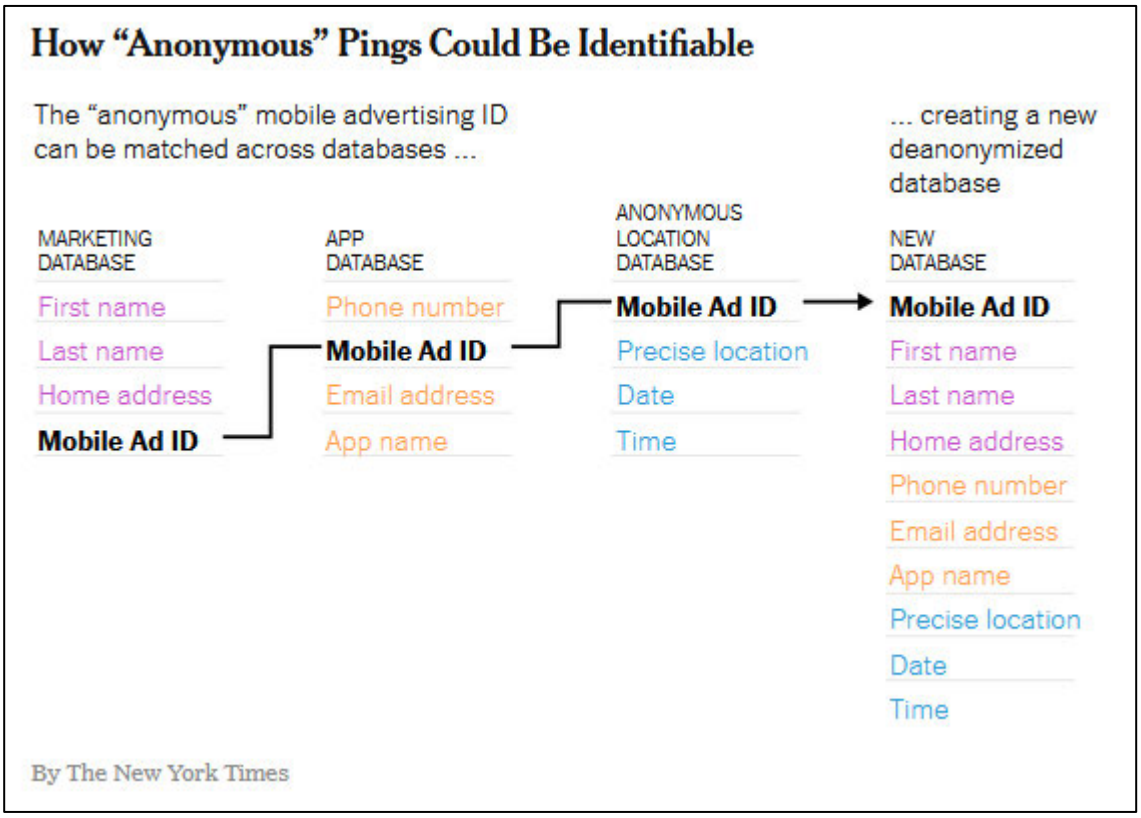
[37] Warzel, C. and Thompson, S. (Feb. 5, 2021), *They Stormed the Capitol. Their Apps Tracked Them.* The New York Times. https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html

The trip to Washington, D.C.

The day of the protest



149. *The New York Times* further reported that, by purchasing data from advertisers, it was "quickly able to match more than 2,000 supposedly anonymous devices in the data set [of people in or around the Capitol on the afternoon of January 6, 2021] with email addresses, birthdays, ethnicities, ages and more."



C. Google Sells Account Holders' Private Information

150. Google's release, disclosure, dissemination, transfer, and electronic communication of Account Holders' personal information to participants in Google RTB is a sale of personal information for purposes of advertising.

151. The communication of Account Holders' personal information is made by Google in exchange for money and other valuable consideration.

152. The winning bidder pays for Account Holders' personal information.

153. Participants in Google RTB who do not win a bid to place an ad nevertheless receive Account Holders' personal information in exchange for other valuable consideration. This includes their continued participation in Google RTB, *i.e.,* the continued ability to receive, review, retain and bid on Account Holders' personal information.

154. Moreover, even participants that do not submit a bid to advertise directly to an Account Holder still receive access to that Account Holder's personal information via the Google RTB. This is a benefit and encourages them to participate in the auction.

155. All of the data transferred by Google is associated with multiple unique persistent identifiers. After the data leaves an Account Holder's device, it is sent to Google RTB, which entertains bids from SSPs all over the internet as well as bids from Google itself. Those bids are then presented to DSPs (who are acting on behalf of advertisers), also including Google itself. All of these third parties on the Ad Exchange thus have an opportunity to review and analyze the personal information about Account Holders that Google has collected and disseminated through the Bid Request.

156. This directly violates Google's promises to Account Holders that it will not sell their information to advertisers or share the information except in limited circumstances.

1. Plaintiffs Have Identified Hundreds of Companies Who Are Winning Bidders in Google's Ad Exchange Auctions

157. There is no transparency in the process that occurs in Google RTB. Indeed, one of the factors motivating recent antitrust investigations into Google is that Ad Stack markets are opaque, Google has a powerful role in multiple layers of the process, and Google has resisted disclosure of how the auctions operate. Plaintiffs' investigation is ongoing and many of these practices are only now coming to light and being analyzed by experts.

158. Regardless, and relevant here, Google does not tell Account Holders which companies are bidding on, and therefore accessing, their personal information, let alone which companies are winning the auctions.

159. To determine the prevalence of Google RTB in the United States, Plaintiffs retained Professor Wilson of the Khoury College of Computer Sciences at Northeastern University. Plaintiffs asked Professor Wilson to identify the raw number of publishers (those websites who are selling ad space on the Google Ad Exchange) that use the Google RTB in the United States.

160. Professor Wilson determined the precise number of publishers in the Google RTB by downloading the data Google publishes at https://storage.googleapis.com/adx-rtb-dictionaries/sellers.json. Professor Wilson determined that 1,298,541 publishers were identified by Google as participating in the Google RTB to sell their ad space. Of the approximately 1.3 million RTB publishers, Professor Wilson determined that only 172,849 (13.31 percent) were publicly disclosed by Google. Google marked the remainder as anonymous.

161. Professor Wilson also researched the scope of the RTB participants who won auctions in an experiment and concluded that there are *at least* 229 different advertisers to whom Google discloses Account Holders' personal information. Among the companies who did not win the auction but to whom Google disclosed Account Holders' personal information were Amazon, Facebook, Twitter, Taboola, Wayfair, Yahoo, and eBay. The list also included hundreds of companies American consumers have likely never heard of. Google solder and shared Account Holder personal information to each of these companies.

162. Professor Wilson's effort to identify these participants through the creation and deployment of massive web-crawling scripts is only necessary because Google is not required to publish such information to American consumers. However, other data protection regimes do require at least some transparency into who is buying Account Holders' personal information. Disclosures and reports from those other jurisdictions indicate that Professor Wilson's report may dramatically underestimate participation in Google RTB and the number of entities to which Google sells user personal information.

163. For example, European law requires Google to identify all companies with which it shares personal data in the European Economic Area. The published list includes 833 companies, including well-known companies like Amazon, Facebook, Twitter, Microsoft (LinkedIn), Netflix, Adobe, Oracle, Salesforce, and eBay, as well as hundreds of little-known companies such as Betgenius, Neustar, and Outbrain.[38]

164. A September 2020 study submitted to the Irish Data Protection Commission estimated that an estimated 13.5 million websites participated in the Google RTB and 2,182 companies directly received Google RTB data.[39]

2. Google's Promises Versus Google's Actions

165. The following chart compares Google's promises with its actions:

What Google Promises	What Google Does
"[W]e never share [personal] information with advertisers, unless you ask us to." *How our business works*, Ex. 5 at 1.	Google shares Account Holders' personal information, including information that is tied to Account Holders' unique identifiers, with Google RTB participants for the purpose of targeted advertising. Google does so without Account Holders' consent.
"We don't share information that personally identifies you with advertisers[.]" *Google Privacy Policy*, *e.g.*, Ex. 15 at 5; Ex. 20 at 6.	
"We do not share your personal information with companies, organizations, or individuals outside of Google except…[1)] With your consent … [3)] With domain	

[38] https://support.google.com/admanager/answer/9012903

[39] Dr. Johnny Ryan, Submission to the Irish Data Protection Commission, Irish Council for Civil Liberties (Sept. 21, 2020) https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf at 16-17.

administrators… [3)] For external processing … and [4)] For legal reasons[.]" *Google Privacy Policy*, *e.g.*, Ex. 15 at 11-12; Ex. 20 at 11-12.	
"[R]emember, we never share any of this personal information with advertisers." *We do not sell your personal information to anyone.*, Ex. 23 at 2.	
"We don't sell your personal information to anyone." *How our business works*, Ex. 5 at 1.	
"We don't share information that personally identifies you with our advertising partners, such as your name or email, unless you ask us to share it." *Who are Google's Partners?*, Ex. 21 at 2.	While Google may not directly provide Account Holders' names or email, Google does share their unique identifiers, provides cookie matching services to assist in identification of Account Holders, and encourages Google RTB participants to store user lists and hashed keys that enables them to reidentify Account Holders whose names and emails are known to participants.
"Without identifying you personally to advertisers or other third parties, we might use data that includes your searches and location, websites and apps that you've used, videos and ads you've seen, and basic information that you've given us, such as your age range and gender." *We do not sell your personal information to anyone.*, Ex. 23 at 1.	
"We give advertisers data about their ads' performance, but we do so without revealing any of your personal information. At every point in the process of showing you ads, we keep your personal information protected and private." *We do not sell your personal information to anyone.*, Ex. 23 at 1.	Google not only fails to protect personal information, but rather directly provides it to Google RTB participants and enables participants to de-anonymize personal information with cookie matching services.
"Privacy is personal, which makes it even more vital for companies to give people clear, individual choices around how their data is used." *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, Ex. 25 at 1.	Google does not provide Account Holders with clear individual choices about how their data is used; rather, Google provides misinformation and broken promises about user privacy and fails to disclose that Account Holders' personal information is being sold on Google RTB.
"[P]rivacy cannot be a luxury good offered only to people who can afford to buy premium products and services. Privacy must be equally available to everyone in the world." *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, Ex. 25 at 1.	Google does not make "privacy equally available." Instead, it targets its own Account Holders, making privacy unavailable to them by subversively revealing their personal information thousands of times per second to millions of Google RTB participants. Only Google and Google RTB participants, not Account Holders, profit.

"To make privacy real, we give you clear, meaningful choices around your data. All while staying true to two unequivocal policies: that Google will never sell any personal information to third parties; and that you get to decide how your information is used." *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, Ex. 25 at 1.	Google does not disclose what it is doing with Account Holders' data and gives Account Holders no choice about whether their personal information is sold at the Google RTB auctions.
"Advertisers do not pay us for personal information[.]" *How our business works*, Ex. 5 at 1.	Through Google RTB, advertisers in fact do pay Google for advertising the value of which is directly tied to the disclosure of Account Holders' personal information.
"We never sell your personal information, and give you controls over who has access." *Your privacy is protected by responsible data practices*, Ex. 24 at 2.	Google sells Account Holders' personal information on Google RTB, a process that is invisible to Account Holders and in which their consent is not solicited prior to sale.
"At every point in the process of showing you ads, we keep your personal information protected with industry-leading security technologies." *How our business works*, Ex. 5 at 2.	Google reveals Account Holders' personal information in the Google RTB Bid Requests and provides cookie matching tools that enable participants to match Account Holders' personal information with individual profiles the participants already has.
"Privacy is core to how we build our products, with rigorous privacy standards guiding every stage of product development. Each product and feature adheres to these privacy standards, which are implemented through comprehensive privacy reviews." *Your privacy is protected by responsible data practices*, Ex. 24 at 4.	Google's core practice is building Account Holder profiles and monetizing those profiles through, among other things, the Google RTB, where Google sells Account Holders' personal information to facilitate targeted advertising, all the while making false promises of privacy to Account Holders.
"We also never use your emails, documents, photos, or sensitive information like race, religion, or sexual orientation, to personalize ads to you." *How our business works*, Ex. 5 at 2.	Google targets Account Holders based on their sensitive information, like race, religion, sexual orientation, and health. Google does this by collecting Account Holders' browsing information to determine whether Account Holders' fall within certain consumer categories, known as verticals and segments. These consumer categories include sensitive categories related to race, religion, sexual orientation, and health. This information is then shared with Google RTB participants to facilitate targeted advertising based on those sensitive categories. Google RTB participants are then able to bid on the ability to serve ads to Account Holders, including the ability to serve personalized ads based on specific sensitive information.
"We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health." *Google Privacy Policy*, *e.g.,* Ex. 15 at 5; Ex. 20 at 6.	
"We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers [hyperlink] that use our services." *Google Privacy Policy, e.g.*, Ex. 15 at 22; Ex. 20 at 30.	

"Advertisers can't use sensitive interest categories to target ads to users or to promote advertisers' products or services." *Personalized Advertising*, Ex. 22 at 2.	
"Personal hardships: Because we don't want ads to exploit the difficulties or struggles of users, we don't allow categories related to personal hardships." *Personalized Advertising*, Ex. 22 at 2.	Google groups Account Holders into verticals and segments and facilitates targeted advertising based on these verticals and segments, which include those related to personal hardships, like health issues (e.g., depression, eating disorders, infectious diseases, learning & developmental disabilities), financial hardship (e.g., bankruptcy, debt collection & repossession, short-term loans & cash), and difficult interpersonal circumstances (e.g., troubled relationships, divorce & separation).
"Identity and belief: Because we want ads to reflect a user's interests rather than more personal interpretations of their fundamental identity, we don't allow categories related to identity and belief, some of which could also be used to stigmatize an individual." *Personalized Advertising*, Ex. 22 at 2.	Google allows advertisers to target messages to Account Holders based on verticals and segments related to identity and belief, including religion (e.g., Judaism, Islam) and identity (e.g., lesbian, gay, bisexual & transgender).
"Sexual interests: Because we understand that sexual experiences and interests are inherently private, we don't allow categories related to sexual interests." *Personalized Advertising*, Ex. 22 at 2.	Google allows advertisers to target messages to Account Holders based on verticals and segments related to sexual interests (e.g., sexual enhancement).

"The following sensitive interest categories can't be used by advertisers to target ads to users or promote advertisers' products or services": • "Restricted drug terms … [including] Prescription medications and information about prescription medications"; • "Personal hardships … [including] health conditions, treatments, procedures, personal failings, struggles, or traumatic personal experiences"; • "Personal health content, which includes: []Physical or mental health conditions, including diseases, sexual health and chronic health conditions, which are health conditions that require long-term care or management[; and] Products, services, or procedures to treat or manage chronic health conditions, which includes over-the-counter medications and medical devices"; • "Relationships [including] Personal hardships with family, friends, or other interpersonal relationships"; • "Sexual orientation"; • "Personal race or ethnicity" and • "Personal religious beliefs" *Personalized Advertising*, Ex. 22 at 2-5.	Google allows advertisers to target messages to Account Holders sorted by Google into verticals and segments related to verticals and segments related to the following categories and examples within each: Prescription medications: Drugs & Medications Personal Hardships & Personal Health Content: AIDS & HIV; Cancer; Eating Disorders; Genetic Disorders; Infectious Diseases; Neurological Conditions; Learning & Developmental Disabilities; Autism Spectrum Disorders; Obesity; Skin Conditions; Counseling Services; Depression; Fertility; Male Impotence; Sexual Enhancement; Sexually Transmitted Diseases; Drug & Alcohol Treatment; Steroids & Performance Enhancing Drugs; Anxiety & Stress; Counseling Services; Drugs & Medications; Troubled Relationships; Divorce & Separation; Bankruptcy; Debt Collection & Repossession; Short-Term Loans & Cash Sexual Orientation: Lesbian, Gay, Bisexual & Transgender Race/Ethnicity: African-Americans; Arabs & Middle Easterners; South Asians & Diaspora; Southeast Asians & Pacific Islanders; Eastern Europeans; Native Americans; Jewish Culture; Latinos & Latin-Americans Religious Beliefs: Buddhism; Christianity; Hinduism; Islam; Judaism

D. Google's Improper Sale of Personal Information Is a Serious Invasion of the Privacy and Is Highly Offensive

166. Article I, § 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." The phrase "and privacy" was added by the "Privacy Initiative" adopted by California voters in 1972.

167. The right to privacy in California's constitution creates a right of action against private entities. The principal purpose of this constitutional right was to protect against unnecessary

information gathering, use and dissemination by public and private entities, including computer-stored and -generated dossiers and cradle-to-grave profiles on every American.

168. In its public statements, Google pays lip service to the need to protect the privacy of Internet communications. For example, on June 6, 2016, a coalition of technology companies and privacy advocates came together to oppose Congressional efforts to expand government surveillance of online activities through the Senate's Intelligence Authorization Act for Fiscal Year 2017 and Senator Cornyn's proposed amendments to the ECPA.

169. The joint letter, signed by the ACLU, Amnesty International and others, was also signed by Google. These organizations and companies argued (correctly) that obtaining sensitive information about Americans' online activities without court oversight was an unacceptable privacy harm because it "would paint an incredibly intimate picture of an individual's life" if it included "browsing history, email metadata, location information, and the exact date and time a person signs in or out of a particular online account."[40]

170. The letter further posited that the proposed online surveillance could "reveal details about a person's political affiliation, medical conditions, religion, substance abuse history, sexual orientation" and even physical movements. The letter concluded that online surveillance raises "civil liberties and human rights concerns."

171. Google has publicly declared that non-consensual electronic surveillance is "dishonest" behavior. For example, Google's Update to its "Enabling Dishonest Behavior Policy" (effective August 11, 2020) restricted advertising for spyware and surveillance technology. The updated policy purports to "prohibit the promotion of products or services that are marketed or targeted with the express purpose of tracking or monitoring another person or their activities without their authorization." Through this amendment, Google explicitly takes the position that nonconsensual surveillance of "browsing history" is "dishonest behavior."[41]

---

[40] June 6, 2016 Joint Letter. Available at http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/06-06-16%20Coalition%20Letter%20to%20Senators%20in%20Opposition%20to%20Expansion%20of%20NSL%20Statute%20on%20ECTRs.pdf

[41] https://support.google.com/adspolicy/answer/9726908?hl=en&ref_topic=29265

172. Google has also publicly declared privacy to be a human right. In 2004, in a letter from Google's founders to shareholders at the IPO (included with the Company's S-1 Registration Statement filed with the SEC), Google declared its goal to "improve the lives of as many people as possible."[42] This letter appears today on Google's website on a page touting the company's commitment to be guided by "internationally recognized human rights standards," including specifically the human rights enumerated in three documents: The Universal Declaration of Human Rights (the "Universal Declaration"); the United Nations Guiding Principles on Business and Human Rights (the "UN Principles"); and the Global Network Initiative Principles (the "GNI Principles").

173. These three documents establish that privacy is a human right and a violation of privacy rights is a violation of human rights. The Universal Declaration declares that no one should be subject to arbitrary interference with privacy, and even declares the right to the protection of laws against such interference. Similarly, the UN Guiding Principles for business identify privacy as a human right. The GNI Principles has an entire section dedicated to privacy that begins: "Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age."[43]

174. Finally, although not mentioned on Google's website, in 1992 the United States ratified the International Covenant on Civil and Political Rights, a human rights treaty that guarantees privacy rights in Article 17.

E. Google Faces Numerous Regulatory and Governmental Agency Investigations for RTB Privacy Concerns

175. In May 2019, the Irish Data Protection Commission opened an investigation into Google RTB after receiving complaints from the Irish Council for Civil Liberties (ICCL) and other groups about the disclosure of personal information in Google RTB. This investigation remains ongoing.

[42] https://about.google/intl/ALL_my/human-rights/

[43] https://globalnetworkinitiative.org/gni-principles/

176. The U.K.'s Information Commissioner's Office (ICO) has also opened an investigation into the privacy risks associated with RTB exchanges, including Google RTB. In a June 2019 report published by the ICO, the organization noted the following concerns:[44]

> 1. Processing of non-special category data is taking place unlawfully at the point of collection due to the perception that legitimate interests can be used for placing and/or reading a cookie or other technology . . . .
>
> 6. The profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individuals' knowledge.
>
> 7. Thousands of organisations are processing billions of bid requests in the UK each week with (at best) inconsistent application of adequate technical and organisational measures to secure the data in transit and at rest, and with little or no consideration as to the requirements of data protection law about international transfers of personal data.
>
> 8. There are similar inconsistencies about the application of data minimisation and retention controls.
>
> 9. Individuals have no guarantees about the security of their personal data within the ecosystem.

177. The ICO recently announced it would be reopening this investigation after temporarily suspending it to respond to the COVID-19 pandemic.[45] The ICO noted that in response to its ongoing investigation, Google "will remove content categories, and improve its process for auditing counterparties."[46] Despite these vague promises, Google has not stopped disclosing users' personal information.

178. The Belgian Data Protection Commission likewise has opened an investigation into privacy risks on RTB exchanges. In October 2020, the Belgium privacy authority issued an internal report focusing on the online ad auctions and identifying as a core problem, how online-ad bidding

---

[44] *Update report into adtech and real time bidding*, Information Commissioner's Office, June 20, 2010, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

[45] Simon McDougall, *Adtech - the reform of real time bidding has started and will continue*, Jan. 17, 2020, https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/.

[46] *Id.*

systems "collect personal data when a user hasn't consented to share it."[47] The report "also took issue with the collection of 'sensitive category' data about users—such as race, sexuality, health status or political leaning—without their consent."[48] This investigation is ongoing.[49]

179. In addition, dozens of complaints have been filed by civil liberties groups against Google and IAB over privacy abuses arising from real-time bidding. The list of countries where these complaints have been filed with governmental regulators includes: Bulgaria, Croatia, Cyprus, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, and Spain.[50] Investigations regarding these complaints are ongoing.

180. Further, as detailed above, in a July 2020 letter, Senator Wyden and other members of Congress urged the FTC to examine the privacy dangers of RTB exchanges. The letter explains that "hundreds of participants in these auctions receive sensitive information about the potential recipient of the ad—device identifiers and cookies, location data, IP addresses, and unique demographic and biometric information such as age and gender. Hundreds of potential bidders receive this information, even though only one—the auction winner—will use it to deliver an advertisement." The Congressional letter further cites to Mobilewalla as an example, explaining how Mobilewalla used bidstream data, location, and inferred race data to profile participants in recent Black Lives Matter protests.[51]

[47] Patience Haggin and Sam Schechner, *European Regulator Turns Up Heat on Ad Tactics Used by Google and Rivals*, WSJ (Oct. 16, 2020) https://www.wsj.com/articles/european-regulator-turns-up-heat-on-ad-tactics-used-by-google-and-rivals-11602872300.

[48] *Id.*

[49] Natasha Lomas, *Google and IAB adtech targeted with more RTB privacy complaints*, TechCrunch, Dec. 10, 2020, https://techcrunch.com/2020/12/10/google-and-iab-adtech-targeted-in-latest-batch-of-rtb-privacy-complaints/.

[50] https://privacyinternational.org/examples/4349/cso-coalition-files-complaints-against-google-and-iab-member-companies-six-eu-states; https://brave.com/rtb-updates/.

[51] Wyden FTC Letter.

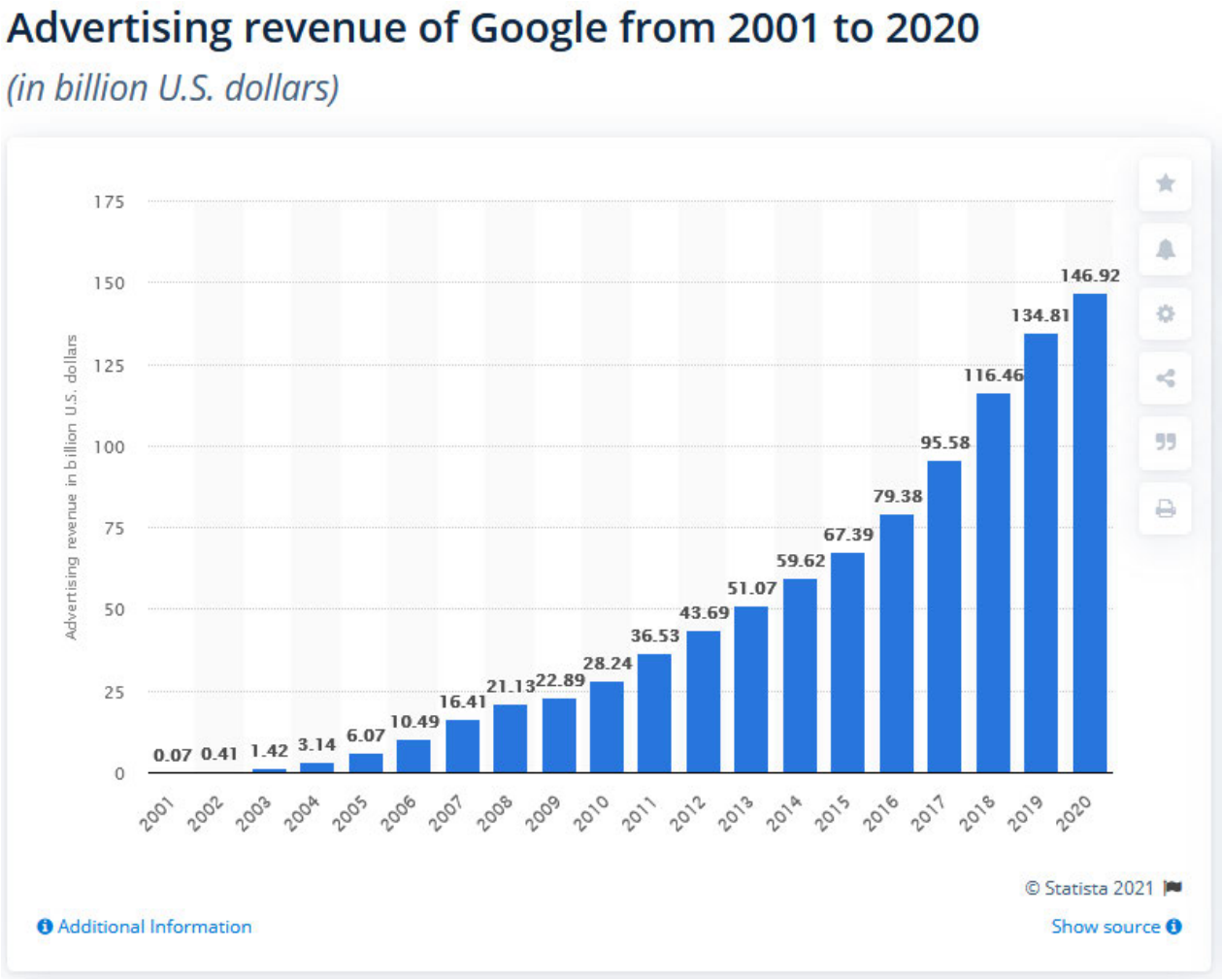
181. This growing list of governmental entities that have opened investigations into the ad exchange process highlights the threat Account Holders face of their personal information being collected through Google RTB.

F. Google Has Been Unjustly Enriched

182. Google's $1 trillion business was built entirely on monetizing the value of Internet users' personal information.

183. The value of Plaintiffs' personal information to Google is demonstrated in part by Google's advertisement revenue during the relevant time period. Google reported $146.9 billion in advertising revenue in 2020, $134.8 billion in 2019, $116.3 billion in 2018, $95.4 billion in 2017, and $79.4 billion in 2016.[52] This translates to 83% of Google's total revenues in 2019, 85% in 2018, 86% in 2017 and 88% in 2016.[53] While not all of that value is unjustly derived from the specific information collected by Google here, some portion of it is. Shown graphically below, Google's annual advertising revenue has increased over five hundred percent since 2008.[54]

[52] *2018 Annual Report*, Alphabet Inc. (Feb. 4, 2019), https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm (hereinafter "2018 Annual Report").
[53] 2019 Annual Report, Alphabet Inc. (Feb. 3, 2020), https://www.sec.gov/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm (hereinafter "2019 Annual Report"); 2018 Annual Report.
[54] J. Clement, *Advertising revenue of Google from 2001 to 2019*, statista (Feb. 5, 2020), https://www.statista.com/statistics/266249/advertising-revenue-of-google/.

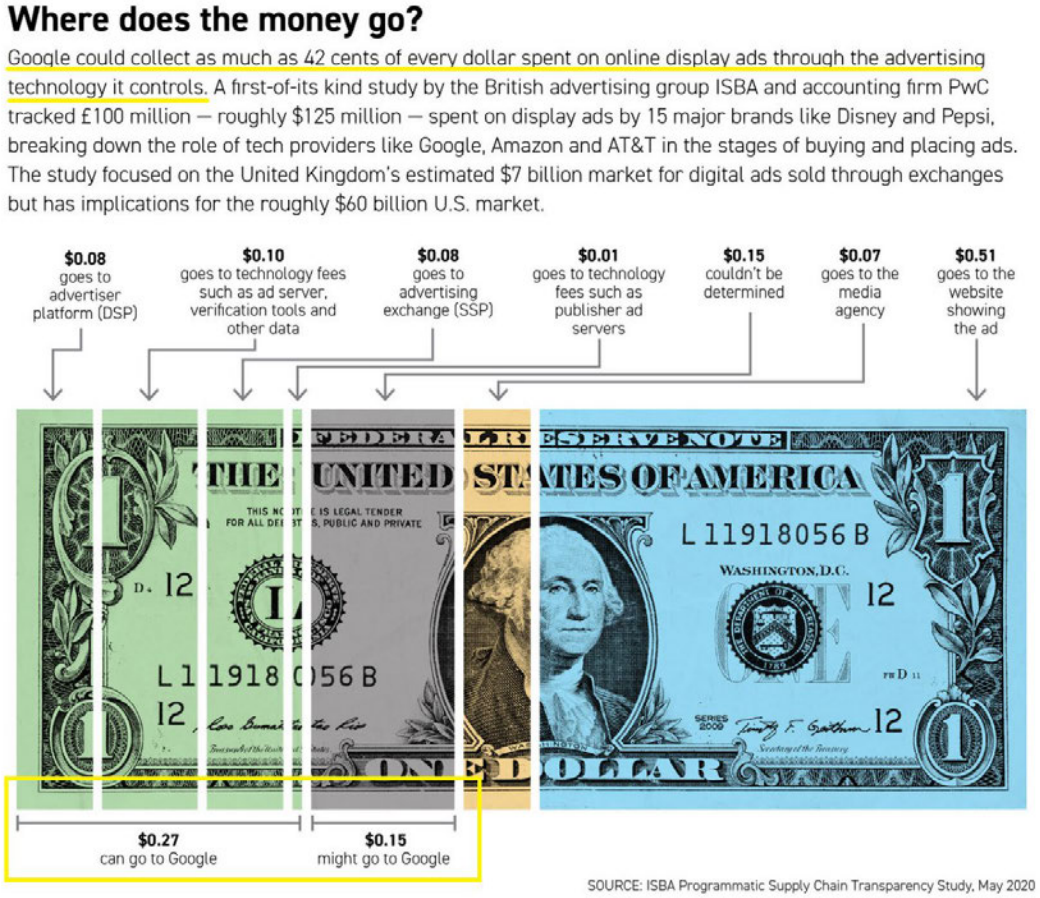


184. The collection of Account Holders' personal information has facilitated the revenues of Google's Network Members' properties, which include ads placed through AdMob, AdSense, DoubleClick AdExchange. Google reported the following revenues from Google Network Members' properties: $21.5 billion in 2019, $20 billion in 2018, $17.6 billion in 2017, and $15.6 billion in 2016.[55] Google reports "strength in both AdMob and AdManager" primarily led to the $2.4 billion increase in Google Network Members' properties revenues from 2017 to 2018.[56]

[55] 2019 Annual Report; 2018 Annual Report.

[56] 2019 Annual Report.

185. The fact of the advertising auctions themselves confirms that the personal information Google sells to RTB participants has economic value. A recent article published by Politico discussed one study that found that Google makes as much as 42 cents for each dollar spent on advertising on its platform.[57]



186. A 2019 study co-authored by Robert J. Shapiro and Siddartha Aneja, titled *Who Owns America's Personal Information and What is it Worth?*, calculated the value of Americans' personal information gathered and used by Google: $15.3 billion in 2016, $18.1 billion in 2017, and $21.5 billion in 2018. [58]

[57] Leah Nylen, *Google dominates online adds – and DOJ may be ready to pounce*, Politico (June 4, 2020), https://www.politico.com/news/2020/06/04/google-doj-ads-302576.

[58] Robert Shapiro and Siddhartha Aneja, *Who Owns Americans' Personal Information and What Is It Worth?*, Future Majority (April 2019), *available at* http://www.sonecon.com/docs/studies/Report_on_the_Value_of_Peoples_Personal_Data-Shapiro-Aneja-Future_Majority-March_2019.pdf. Shapiro is a Senior Policy Fellow at the Georgetown University McDonough

Table 1. The Value of Americans' Personal Information Gathered and Used by Major Internet Platforms, Data Brokers, Credit Card and Healthcare Data Companies 2016-2018 ($ billions)

Platform	2016	2017	2018	Increase
Major Internet Platforms				
Google	$15,303.6	$18,132.4	$21,453.5	40.2%
Facebook	$6,432.4	$9,344.4	$11,882.0	84.7%
Amazon	$582.4	$920.4	$2,397.2	311.6%
Microsoft	$1,736.8	$1,944.8	$2,339.4	34.7%
Oath (Verizon)	$1,830.4	$1,872.0	$1,917.8	4.8%
Twitter	$707.2	$608.4	$728.2	2.9%
Other	$10,951.2	$14,180.4	$17,045.7	55.7%
Subtotal	**$37,544.0**	**$47,002.8**	**$57,763.9**	**53.9%**
Major Data Brokers				
Axciom	$804.0	$824.6	$1,053.0	31.0%
CoreLogic	$1,755.9	$1,664.7	$1,650.5	- 6.0%
Epsilon	$2,062.4	$2,174.3	$2,080.2	0.08%
Equifax	$1,938.7	$2,026.9	$2,066.4	6.6%
Experian	$2,412.5	$2,597.5	$3,070.7	27.3%
FICO	$572.9	$596.6	$681.4	18.9%
Harte-Hanks	$348.6	$330.9	$249.8	28.3%
RELX	$1,910.3	$1,973.6	$2,061.9	7.9%
Transunion	$1,452.2	$1,636.2	$1,934.3	33.2%
Subtotal	**$13,257.6**	**$13,825.3**	**$14,848.2**	**12.0%**
Credit Card Firms				
MasterCard	$1,010.1	$1,185.4	$1,418.1	40.4%
American Express	$238.2	$279.6	$334.5	40.4%
Subtotal	**$1,248.3**	**$1,465.0**	**$1,752.6**	**40.4%**
Healthcare Data Firm				
IQVIA	$443.4	$1,478.1	$1,681.5	379.2%
TOTAL	**$52,493.3**	**$63,771.2**	**$76,046.2**	**44.9%**

School of Business and, among other past positions, served as the U.S. Under-Secretary of Commerce for Economic Affairs under President Clinton.

187. Shapiro and Aneja further predicted that Americans' personal information gathered and used by Google would be worth $30.1 billion in 2020, and $42.2 billion in 2022.

Table 2. Projected Value of Americans' Personal Information Gathered and Used by Major Internet Platforms, Data Brokers, Credit Card and Healthcare Data Companies 2020 and 2022 ($ billions)

Platform	2018	2020	2022
Major Internet Platforms			
Google	$21,453.5	$30,077.2	$42,167.3
Facebook	$11,882.0	$21,948.6	$40,543.7
Amazon	$2,397.2	$9,867.1	$40,613.5
Microsoft	$2,339.4	$3,151.9	$4,246.6
Oath (Verizon)	$1,917.8	$2,010.4	$2,107.5
Twitter	$728.2	$749.7	$771.7
Other	$17,045.7	$26,531.7	$41,296.8
Subtotal	**$57,763.9**	**$94,336.5**	**$171,747.1**
Major Data Brokers			
Axciom	$1,053.0	$1,379.1	$1,806.2
CoreLogic	$1,650.5	$1,551.4	$1,458.3
Epsilon	$2,080.2	$2,098.2	$2,116.3
Equifax	$2,066.4	$2,202.5	$2,347.6
Experian	$3,070.7	$3,908.5	$4,974.8
FICO	$681.4	$810.5	$963.9
Harte-Hanks	$249.8	$179.0	$128.3
RELX	$2,061.9	$2,225.5	$2,402.2
Transunion	$1,934.3	$2,576.5	$3,431.8
Subtotal	**$14,848.2**	**$16,933.1**	**$19,629.3**
Credit Card Firms			
MasterCard	$1,418.1	$1,991.0	$2,795.3
American Express	$334.5	$469.6	$659.3
Subtotal	**$1,752.6**	**$2,460.6**	**$3,454.5**
Healthcare Data Firm			
IQVIA	$1,681.5	$2,177.6	$2,820.1
TOTAL	**$76,046.2**	**$115,907.8**	**$197,651.1**

188. The intergovernmental economic organization the Organization for Economic Cooperation and Development ("OECD") has issued numerous publications discussing how to value data such as that which is the subject matter of this Complaint. For example, as early as 2013, the OECD published a paper titled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[59] More recently, the OECD issued a study

[59] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013), http://dx.doi.org/10.1787/5k486qtxldmq-en.

recognizing that data is a key competitive input not only in the digital economy but in all markets: "Big data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[60]

189. The Google RTB relies on the disclosure of sufficiently detailed personal information so that bidders can be confident their ads are purchased for the right Account Holders, so that the ads are likelier to be effective. Without personal information, Google RTB would not provide sufficient information for bidders to make an informed bid, and prices for the bids would be lower.

190. There is also a market incentive for companies to participate in an RTB system solely for the purpose of compiling consumer data for further sale, even if those companies have no intention of placing advertisements. This is because mere participation in an RTB enables participants to receive Account Holders' personal information even if they never prevail on, or even submit, a bid. Participants can thus harvest information through an RTB and can resell it to make money.

191. In her book *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshana Zuboff notes Google's early success monetizing account holder data prompted large corporations like Verizon, AT&T and Comcast to transform their business models from fee for services provided to customers to monetizing their users' data—including user data that is not necessary for product or service use, which she refers to as "behavioral surplus."[61] In essence, Professor Zuboff explains that revenue from user data pervades every economic transaction in the modern economy. These revenues reveal that there is a market for this data. Data generated by users on Google's platform has economic value.

192. While the economic value of user data was discovered and leveraged by corporations who pioneered the methods of its extraction, analysis, and use, user data can also have economic value to user themselves. Market exchanges have sprung up where individual users like

[60] *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct. 13, 2013), https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en.

[61] Shoshana Zuboff, The Age of Surveillance Capitalism 166 (2019).

Plaintiffs herein can sell or monetize their own data. For example, Nielsen Computer and Mobile Panel pays certain users for their data.[62] Facebook has launched apps that pay users for their data directly.[63] Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.[64]

193. Indeed, Google once paid users to track their online behaviors:

> Google is building an opt-in user panel that will track and analyze people's online behaviors via an extension to its Chrome browser, called Screenwise. Users that install the plug-in will have the websites they visit and the ways in which they interact with them recorded, and they will then be paid with Amazon gift cards worth up to $25 a year in return.[65]

194. There are other markets for users' personal information. One study by content marketing agency Fractl has found that an individual's online identity, including hacked financial accounts, can be sold for $1,200 on the dark web.[66] These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other users' content, the implication is that there is a market for users to sell their own data.

195. As Professors Acquisti, Taylor and Wagman relayed in their 2016 article "The Economics of Privacy," published in the *Journal of Economic Literature*:

> Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's

---

[62] Kevin Mercadante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (March 16, 2021), https://wallethacks.com/apps-for-selling-your-data/.

[63] Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 30, 2019), https://www.cnbc.com/2019/01/29/Facebook-paying-users-to-install-app-to-collect-data-techcrunch.html

[64] Jacob Kastrenakes, *A New TikTok Clone hit the top of the App Store by Paying users to watch videos*, The Verge (May 29, 2020), https://www.theverge.com/2020/5/29/21274994/zynn-tiktok-clone-pay-watch-videos-kuaishou-bytedance-rival.

[65] Jack Marshall, *Google Pays Users for Browsing Data*, DigiDay (Feb. 10, 2012), https://digiday.com/media/google-pays-users-for-browsing-data/.

[66] Maria LaMagna, *The sad truth about how much your Facebook data is worth on the dark web*, MarketWatch (June 6, 2018), https://www.marketwatch.com/story/spooked-by-the-Google-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20.

> age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.[67]

196. While the exact value of users' personal information in this action will be a matter for expert determination, it is clear that Google has been unjustly enriched by the practices described herein.

G. Plaintiffs' Personal Information is Property Under California Law

197. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications.

198. California courts have recognized the lost "property value" of personal information, thus Plaintiffs and Account Holders have a property interest in their own data and personal information.

199. Accordingly, personal information, including websites visited by Plaintiffs and Account Holders, is property under California law.

200. Property includes intangible data, including the very specific data at issue here that Google is taking despite promising Plaintiffs and Account Holders it would not do so—personal information including Internet communications history and personally identifiable information.

201. Recent changes in California law have confirmed that individuals have a property interest in their information. In 2018, California enacted the California Consumer Privacy Act. Among other provisions, the CCPA permits businesses to purchase consumer information from consumers themselves (Cal. Civ. Code § 1798.125(b)(1)) and permits businesses to assess and appraise – *i.e.*, to place a monetary value on – consumer data (Cal. Civ. Code §1798.125(a)(2)).

202. Just last year, Californians passed Proposition 24, the California Privacy Rights Act. In the California General Election Voter Guide, proponents of Proposition 24 made their case for the law by noting specifically that companies use personal information such as a user's location:

---

[67] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Literature 2, at 444 (June 2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf.

"Giant corporations make billions buying and selling our personal information – apps, phones, and cars sell your location constantly."[68] Among other things, passage of the CPRA foreclosed the ability of companies like Google to evade the CCPA by contending they were "sharing," and not "selling," users' personal information. Specifically, the CPRA clarified that the provisions protecting users' data apply equally whether defines its activities as "selling" or "sharing" data. CPRA § 9(a); *see id.* § 4(d)(2) (providing that "service providers" have the same data protection obligations as contractors and third parties).

203. Taking Plaintiffs' and Account Holders' personal information without authorization is larceny under California law regardless of whether and to what extent Google monetized the data, and Plaintiffs and Account Holders have a right to disgorgement and/or restitution damages for the value of the stolen data.

204. Plaintiffs and Account Holders have also suffered benefit of the bargain damages, in that Google shared and sold more data than the parties agreed would be permitted. Those benefit of the bargain damages also include, but are not limited to, (i) loss of the promised benefits of their Google experience; (ii) out-of-pocket costs; and (iii) loss of control over property which has marketable value.

205. In addition, when Plaintiffs and Account Holders became Account Holders, they gained access to Google's various services in exchange for agreeing to Terms of Service that Google drafted. Those terms assured them that Google would not share or sell their personal information without authorization. Now that Google has sold the data without authorization, Plaintiffs and Account Holders are entitled to disgorgement of all such ill-gotten gains.

206. Data brokers and online marketers have developed sophisticated schemes for assessing the value of certain kinds of data, as discussed above. Experts in the field have identified specific values to assign to certain kinds of activity.

207. While Plaintiffs and Account Holders largely knew that Google generates revenue from business by selling advertising directed at them, it was a material term of the bargain that

[68] California General Election Voter Guide, Proposition 24.

Plaintiffs' and Account Holders' personal information would not be shared by Google with third parties.

208. Google did not honor the terms of this bargain.

209. When Google shared and sold Plaintiffs' and Account Holders' personal information, it received direct benefits of payments from those authorized bidders that paid for advertisements based on the personal information.

210. As Google shared and sold Plaintiffs' and Account Holders' personal information beyond that to which Plaintiffs and Account Holders had agreed, Plaintiffs and Account Holders were denied the benefit of a Google experience where they were promised the right to determine the terms and scope of their content and personal information sharing and sale. Thus, through Google's sharing of Plaintiffs' and Account Holders' personal information with hundreds of different third parties, Plaintiffs and Account Holders lost benefits.

211. In order to preserve their privacy, Plaintiffs who now understand at least some of Google's violations—and there remains much to be revealed about Google's actual activities—are presented with the choice of: (i) reducing or ending their participation with Google; or (ii) knowingly accepting less privacy than they were promised. Each of these options deprives Plaintiffs and Account Holders of the remaining benefits of their original bargain. There is no option which recovers it. None of it recaptures the data taken in violation of Google's promises.

212. Further, Plaintiffs and Account Holders were denied the benefit of knowledge that their personal information was being shared by Google. Therefore, they were unable to mitigate harms they incurred because of Google's impermissible sharing and sale of their personal information to hundreds of third parties. That is, Google's lack of transparency prevented and still prevents Plaintiffs' and Account Holders' ability to mitigate.

213. Google knew that it was sharing and selling Plaintiffs' and Account Holders' personal information in violation of its express promises. Yet, Google failed to warn Plaintiffs and Account Holders so that they could take steps to attempt to avoid exposing their personal information.

214. Google also knew that it was not possible for Plaintiffs and Account Holders to use Google without Google sharing or selling their personal information.

215. Google avoided costs it should have incurred because of its own actions—particularly the loss of user engagement which would have resulted from transparent disclosure of Google's actions—and transferred those costs to Plaintiffs and Account Holders. Warning users would have chilled Internet engagement as well as discouraged potential new users from joining.

216. Google was thus not only able to evade or defer these costs but to continue to accrue value for the Company and to further benefit from the delay due to the time value of money. Google has thus transferred all the costs imposed by the unauthorized disclosure of users' content and personal information onto Plaintiffs and Account Holders. Google increased the cost to Plaintiffs and Account Holders of mitigating such unauthorized disclosures by failing to notify them that their personal information had been disclosed so that they could take steps to minimize their exposure on the browser.

217. In addition, Plaintiffs and Account Holders have also suffered from the diminished loss of use of their own personal information, property which has both personal and economic value to them.

218. Plaintiffs' and Account Holders' personal information has value. First, there is transactional, or barter, value to user content and personal information. Indeed, Google has sold the data to other companies – all the while promising users that it would not do so.

219. Second, Plaintiffs' and Account Holders' property, which has economic value, was taken from them without their consent and in contradiction of Google's express promise not to share or sell it to others. There is a market for this data, and it has at minimum a value greater than zero.

220. Plaintiffs and Account Holders were harmed when Google took their property under false pretenses and exerted exclusive control over it, sharing it with and selling it to others without Plaintiffs' and Account Holders' knowledge or authorization.

H. Google's False Privacy Promises are Market-Tested

221. Public polling on Internet tracking has consistently revealed that the overwhelming majority of Americans – 93% – believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]."[69]

222. Google has conducted its own research on the topic and understands that consumers are more likely to trust an Internet company when they believe the company has told them everything about its business practices and when the consumers believe they have control over how the Internet company uses their information.

223. In 2016, Google researcher Martin Ortlieb explained the following in a published research paper titled "Sensitivity of personal data items in different online contexts":[70]

a. "[I]nternet users are reluctant to share personal data items if it is not consciously perceived to be necessary to the primary function of the service;"

b. If the outcome of their Internet activity "can be achieved by sharing only the mandatory data required for that interaction, they do not want to share more."

c. For search providers, like Google, "users do not see a reason, or reasons, for sharing personal data items with a search provider as readily as with social networks and online retailers."

d. "In general, Internet users prefer to keep their online engagement separate – or at least separable – to their real world identity. In other words, they want to keep their personal identity and their virtual identities as disconnected as possible."

e. "Providing re-assurances on the security and secondary use of personal data can help allay these fears."

f. "[A]llowing users control over their digital identity will be key to engaging them at a deeper level."

[69] https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/

[70] Martin Ortlieb and Ryan Garner, *Sensitivity of personal data items in different online contexts*, De Gruyter Oldenbourg (June 3, 2016) available at https://www.degruyter.com/document/doi/10.1515/itit-2016-0016/html (Last Visited Feb. 1, 2021).

g. "Data collected passively – which we have called internet behavior and account linkage in this word – are regarded as highly sensitive in all context scenarios."

h. "[I]f online service providers are collecting data passively they have to be aware that users of their service will consider such data sensitive as privacy concerns become more of a conscious consideration."

i. "The biggest factor reducing the level of data sensitivity in each context scenario is trust."

j. "Trust, when it comes to sharing personal data items, can be generated through positive outcomes (relevant with clear benefits), transparency (no surprises through clear communication), and control (allowing the user to have a say in how and by whom their data is used)."

224. In another paper, Google researchers explained:[71]

> In order to increase users' comfort, . . . first-party companies should adopt more comprehensive communication strategies based on a greater transparency (i.e., what and how data is used or shared), provide more control over the data access to users (e.g., through intuitive settings and an opt-in approach) and clarify the extent of data anonymization before it is being shared.

225. In yet another paper, Google researchers explained:[72]

a. Previous research "has shown that people are more likely to share information if they feel that they have overview knowledge of personal data and are able to act on data controls."

b. "If trust is established through such means, users are ready to share more online and vice versa."

c. "The simple display of all personal data and eventual behavioral traces available can be an overwhelming and anxiety producing experience for users."

d. "Essentially, no one likes to be out of control, so as soon as this becomes apparent or is perceived, users will either execute control or go to places where they have these options."

[71] Igor Bilogrevic and Martin Ortlieb, *"If You Put All The Pieces Together…" – Attitudes Towards Data Combination and Sharing Across Services and Companies*, CHI Conference on Human Factors in Computing Systems (May 2016), available at https://dl.acm.org/doi/pdf/10.1145/2858036.2858432 (Last Visited Feb. 1, 2021).

[72] Martin Ortlieb, et al., *Trust, Transparency & Control in Inferred User Interest Models*, CHI Extended Abstracts on Human Factors in Computing Systems (April 2014).

e. "Recent research also shows that technologies that make individuals feel more in control over the release of personal information may have the unintended consequence of eliciting greater disclosure of sensitive information."

f. "The concept of trust is an extensively studied concept. . . . [T]rust is a social mechanism for reducing complexity. Transposing this to the world of products we could argue that the cumulative experience with a product or brand leads to confidence. In the realm of online services this could mean confidence in a company's practices such as never selling personal data to any third party."

226. Google's research into the value of trust highlights its knowledge of the importance of deceiving Account Holders by giving them the illusion of safety and control over their own data. Google's privacy disclosures reflect this market research by providing Account Holders information to put them at ease. But, as alleged herein, the privacy disclosures are contradicted by the Company's practices.

I. Fraudulent Concealment and Tolling

227. All applicable statutes of limitation have been tolled by Google's knowing and active fraudulent concealment and denial of the facts alleged herein through the time period relevant to this action.

228. Plaintiffs and Account Holders were not informed anywhere in the Terms of Service that Google's advertising services would disclose their personal information; that Google has used their personal information to associate them into verticals and segments that it discloses in the RTB bidding process and/or makes available to participants in that process; that Google enables participants to re-identify Plaintiffs and Account Holders by saving and storing keys that reassociate Plaintiffs' and Account Holders' unique identifiers across platforms and devices; or that Google provides Google RTB participants with cookies that enable them to match information provided by Google during the RTB bidding process with information the participants already have on individuals, including their names and email addresses.

229. Google chooses not to disclose this information precisely because doing so might chill user engagement.

230. Google continues to conceal this information.

231. An average consumer could not reasonably be expected to know or understand how Google is using their data. The developer pages cited herein, while available on the web, are not easily understandable to the average person, and even they do not fully reveal the extent of Google's actions. Indeed, Plaintiffs' counsel had to retain experts to begin to understand Google's practices at issue in this Complaint.

232. Despite reasonable diligence on their part, Plaintiffs remained ignorant of the factual bases for their claims for relief. Google's withholding of material facts concealed the claims alleged herein and tolled all applicable statutes of limitation.

V. CLASS ACTION ALLEGATIONS

233. This is a class action pursuant to Rules 23(a), (b)(2), and (b)(3) (or, alternatively, 23(c)(4)) of the Federal Rules of Civil Procedure on behalf of a Class of all persons residing in the United States with a Google Account who used the Internet on or after Google began using RTB in a manner that disclosed Account Holders' personal information.

234. Excluded from the Class are the Court, Defendant and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling interest.

235. The members of the Class are so numerous that joinder of all members is impracticable.

236. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class include:

a. Whether Google promised not to share personal information with others;

b. Whether Google promised not to sell personal information to others;

c. Whether Google shared Account Holder personal information with others;

d. Whether Google sold Account Holder personal information to others;

e. Whether Google was authorized to disclose Account Holder personal information to others;

f. Whether Google was authorized to sell Account Holder personal information to others;

g. Whether Google breached its contract with Account Holders;

h. Whether Account Holders' Personal Information was improperly sold by Google;

i. Whether Google was unjustly enriched by the unauthorized sales of Account Holders' personal information;

j. Whether Google's actions would be highly offensive to a reasonable person;

k. Whether Google's actions breached the duty of good faith and fair dealing;

l. Whether Google's actions violated the California Unfair Competition Law;

m. Whether Google's actions violated Article I, Section 1 of the California Constitution;

n. Whether Google's actions violated the California Invasion of Privacy Act;

o. Whether Google's actions violated the Electronic Communications Privacy Act;

p. Whether Google's actions violated the Video Privacy Protection Act;

q. Whether and the extent to which injunctive relief is appropriate.

237. Plaintiffs' claims are typical of the claims of other Class Members, as all members of the Class were similarly affected by Google's wrongful conduct in violation of federal and California law as complained of herein.

238. Plaintiffs will fairly and adequately protect the interests of the members of the Class and have retained counsel that is competent and experienced in class action litigation. Plaintiffs have no interest that conflicts with or is otherwise antagonistic to the interests of the other Class Members.

239. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages individual Class and Subclass members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class and Subclass to individually redress the wrongs done to them.

240. There will be no difficulty in management of this action as a class action.

VI. COUNTS

COUNT ONE: BREACH OF CONTRACT

241. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

242. Google's relationship with its account holders is governed by the Google Terms of Service.

243. Since March 31, 2020, the Google Terms of Service incorporated by reference the document titled "How our business works."

244. Through these documents, Google tells account holders:[73]

a. "We don't sell your personal information to anyone."

b. "[W]e never sell your personal information to anyone[.]"

c. "Advertisers do not pay us for personal information, such as your name or email, and we never share that information with advertisers, unless you ask us to [hyperlink]." *Id.*

d. "We also never use your emails, documents, photos, or sensitive information like race, religion, or sexual orientation, to personalize ads to you."

e. "We share reports with our advertisers . . . but we do so without revealing any of your personal information."

f. "At every point in the process of showing you ads, we keep your personal information protected with industry-leading security technologies [hyperlink]."

g. "When you use our products you trust us with your personal information. That's why we never sell your personal information."

245. Since at least May 25, 2018, the Google Privacy Policy has also told account holders:

a. "We don't share information that personally identifies you with advertisers[.]" *E.g.*, Ex. 12 at 5; Ex. 15 at 5.

b. "We don't show you personalized ads based on sensitive categories [hyperlink], such as race, religion, sexual orientation, or health." *E.g.*, Ex. 12 at 5; Ex. 15 at 5.

[73] Ex. 5 at 1-2.

c. Google's Privacy Policy includes a definition of "sensitive categories" that promises: "We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers [hyperlink] that use our services." *E.g.*, Ex. 12 at 21; Ex. 15 at 22.

246. Moreover, since at least March 1, 2012, the Privacy Policy has promised, "We do not share your personal information with companies, organizations, or individuals outside of Google[.]" *E.g.*, Ex. 15 at 11. The Privacy Policy identifies four exceptions to this promise, none of which applies to the allegations herein.[74]

247. Prior to May 2018, Account Holders who created a Google Account were required to agree to both the Terms of Service and the Privacy Policy.

248. From May 2018 to March 31, 2020, while Account Holders were required to agree to only the Terms of Service, the Google Account creation process included a link to the Privacy Policy as a guide to how Google would "process your information."

249. The Terms of Service expressly adopt California substantive law, including California's definition of personal information.

250. Plaintiffs and Class Members accepted Google's offer, have fulfilled their obligations under the contract, and are not in breach of contract.

251. Google has breached and continues to breach its contractual promise to maintain the privacy of Account Holders' personal information by selling and sharing Plaintiffs' and Class Members' personal information through Google RTB.

252. As a result of Google's breach of its contractual obligations, Google was able to obtain the personal property of Plaintiffs and Class Members, earn unjust profits, and cause privacy injury and other consequential damages.

253. Plaintiffs and Class Members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of certain personal

[74] The four exceptions in Google's Privacy Policy state that Google may share personal information with companies, organizations, and individuals outside Google: (1) with the Account Holder's consent; (2) with domain administrators; (3) for external processing; and (4) for legal reasons. *See*, *e.g.*, Ex. 15 at 11-12.

information they agreed to share. As alleged above, this personal information has ascertainable value to be proven at trial.

254. As a result of Google's breach of its contractual promises, Plaintiffs and Class Members are entitled to recover benefit of the bargain damages, unjust enrichment, and nominal damages.

COUNT TWO: BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

255. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

256. Every contract imposes upon each party a duty of good faith and fair dealing in its performance and enforcement.

257. In dealings between Google, Plaintiffs and Class Members, Google is invested with discretionary power affecting the rights of its Account Holders.

258. The terms of Google's contract with Account Holders purport to respect and protect Account Holders' privacy and expressly promise not to sell or share their personal information. Google not only violated these contractual promises, it frustrated the purpose of those terms by specifically and repeatedly selling and sharing Account Holders' data through its RTB process.

259. Moreover, Google made statements concerning the purported privacy of Account Holder data outside of the specific confines of the contracts it drafted and required Account Holders to enter. By explicitly violating these extra-contractual terms and thereby acting in bad faith, Google violated the implied covenant of good faith and fair dealing.

260. On the "How our business works" webpage, Google promises, "[W]hen you use our products you trust us with your personal information. That's why we never sell your personal information and why we give you powerful privacy controls." Ex. 5 at 2.

261. On Google's "Who are Google's Partners" webpage,

a. Google states: "We don't share information that personally identifies you with our advertising partners, such as your name or email, unless you ask us to share it." Ex. 21 at 2.

b. Google identifies seven "partners" that it permits to "collect or receive non-personally identifiable information about your browser or device when you use Google sites and apps," without disclosing the hundreds of auction participants with whom it shares personal information, including highly-sensitive personal information. *Id.* at 1.

262. On Google's "Personalized Advertising" webpage, Google states:

a. "Advertisers can't use sensitive interest categories to target ads to users or to promote advertisers' products or services." Ex. 22 at 2.

b. "Personal hardships: Because we don't want ads to exploit the difficulties or struggles of users, we don't allow categories related to personal hardships." *Id.*

c. "Identity and belief: Because we want ads to reflect a user's interests rather than more personal interpretations of their fundamental identity, we don't allow categories related to identity and belief, some of which could also be used to stigmatize an individual." *Id.*

d. "Sexual interests: Because we understand that sexual experiences and interests are inherently private, we don't allow categories related to sexual interests." *Id.*

263. On the same webpage, under the header "Prohibited Categories," Google states: "The following sensitive interest categories can't be used by advertisers to target ads to users or to promote advertisers' products or services" (*Id.* at 2):

a. Restricted drug terms – "Prescription medications and information about prescription medications, unless the medication and any listed ingredients are only intended for animal use and are not prone to human abuse or other misuse." *Id.* at 3.

b. "Personal hardships – We understand that users don't want to see ads that exploit their personal struggles, difficulties, and hardships, so we don't allow personalized advertising based on these hardships. Such personal hardships include health conditions, treatments, procedures, personal failings, struggles, or traumatic personal experiences. You also can't impose negativity on the user." *Id.*

c. "Health in personalized advertising [including] Physical or mental health conditions, including diseases, sexual health, and chronic health conditions, which are health conditions that require long-term care or management[;] products, services, or procedures to treat or manage chronic health conditions, which includes over-the-counter medications and medical devices[;] any health issues associated with intimate body parts or functions, which includes genital, bowel, or urinary health[;] invasive medical procedures, which includes cosmetic surgery[;] Disabilities, even when content is oriented toward the user's primary caretaker. Examples [include] Treatments for chronic health conditions like diabetes or arthritis, treatments for sexually transmitted diseases, counseling services for mental health issues like depression or anxiety, medical devices for sleep apnea like CPAP machines, overt-the-counter medications for yeast infections, [and] information about how to support your autistic child." *Id.*

d. "Relationships in personalized advertising [including] Personal hardships with family, friends, or other interpersonal relationships[.] Examples [include] divorce services, books about coping with divorce, bereavement products or services, family counseling services[.]" *Id.* at 4.

e. "Sexual orientation in personalized advertising [including] lesbian, gay, bisexual, questioning, or heterosexual orientation[.] Examples [include] information about revealing your homosexuality, gay dating, gay travel, information about bisexuality." *Id.* at 4-5.

f. "Personal race or ethnicity." *Id.* at 5.

g. "Personal religious beliefs." *Id.*

264. On Google's "Your privacy is protected by responsible data practices" webpage, Google states:

a. "Data plays an important role in making the products and services you use every day more helpful. We are committed to treating that data responsibly and protecting your privacy with strict protocols and innovative privacy technologies." Ex. 24 at 1.

b. That it uses "advanced privacy technologies [to] help keep your personal information private." *Id.* at 3.

c. "We are continuously innovating new technologies that protect your private information without impacting your experiences on our products." *Id.*

d. "We use leading anonymization techniques to protect your data while making our services work better for you." *Id.* at 3-4.

e. "Privacy is core to how we build our products, with rigorous privacy standards guiding every stage of product development. Each product and feature adheres to these privacy standards, which are implemented through comprehensive privacy reviews." *Id.* at 4.

265. On Google's "We do not sell your personal information to anyone" webpage, Google states:

a. "We do not sell your personal information to anyone." Ex. 23 at 1.

b. "Without identifying you personally to advertisers or other third parties, we might use data that includes your searches and location, websites and apps that you've used, videos and ads that you've seen, and basic information that you've given us, such as your age range and gender." *Id.*

c. "We give advertisers data about their ads' performance, but we do so without revealing any of your personal information. At every point in the process of showing you ads, we keep your personal information protected and private." *Id.*

d. "[R]emember, we never share any of this personal information with advertisers." *Id.* at 2.

266. On Google's "Your privacy is protected by responsible data practices" webpage, Google states:

a. "Your privacy is protected by responsible data practices." Ex. 24 at 1.

b. "We never sell your personal information, and give you controls over who has access." *Id.* at 2.

c. "We are committed to protecting your data from third parties. That's why it's our strict policy to never sell your personal information to anyone." *Id.*

d. "We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to." *Id.* at 1-2.

267. Google's CEO Sundar Pichai publicly stated:

a. "We do not and would never sell consumer data." Pichai, *supra* note 10.

b. "To make privacy real, we give you clear, meaningful choices around your data. All while staying true to two unequivocal policies: that Google will never sell any personal information to third parties; and that you get to decide how your information is used." Ex. 25 at 1.

268. Google's sharing and selling of Plaintiffs' and Class Members' personal information with other companies:

a. Was objectively unreasonable given Google's numerous privacy promises both within and outside the confines of the terms it forced Account Holders to agree to in order to become Account Holders;

b. Evaded the spirit of the bargain made between Google, Plaintiffs and Class Members; and

c. Abused Google's power to specify terms in the contract.

269. Google's sharing, sale, and use of Plaintiffs' and Class Members' sensitive personal information for purposes of targeted advertising through Google RTB:

a. Evaded the spirit of the bargain made between Google, Plaintiffs and Class Members; and

b. Abused Google's power to specify terms in the contract.

270. Google's failure to inform Plaintiffs and Class Members of its conduct in Google RTB and failure to give Plaintiffs and Class Members privacy controls to prevent the sale and sharing of their personal information in Google RTB was objectively unreasonable and evaded the spirit of the bargain made between Google, Plaintiffs and Class Members

271. Google's use of Plaintiffs' and Class Members' personal information to target them and enable other companies to add to their own user profiles was in bad faith, and promising Plaintiffs' and Class Members' personal information would not be disclosed induced them to share more information with Google.

272. As a result of Google's misconduct and breach of its duty of good faith and fair dealing, Google was able to obtain the personal property of Plaintiffs and Class Members, earn unjust profits, and cause privacy injury and other consequential damages.

273. As a result of Google's bad faith breach of its contractual and extra-contractual promises, Plaintiffs and Class Members are entitled to recover benefit of the bargain damages, unjust enrichment damages in the form of restitution measures by either unearned profits or a reasonable royalty value, and nominal damages.

COUNT THREE: VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq.*

274. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

275. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

276. Google is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

277. Google violated the UCL by engaging in the following unlawful, unfair, and deceptive business acts and practices:

a. Violating its Terms of Service, knowingly and willfully or negligently and materially, in violation of Cal. Bus. & Prof. Code § 22576;

b. Violating the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 and 2701, *et seq.*;

c. Violating the Video Privacy Protection Act, 18 U.S.C. § 2710, *et seq.*;

d. Violating the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;

e. Violating the California Computer Data Access and Fraud Act, Cal. Penal Code § 502;

f. Committing Statutory Larceny, Cal. Penal Code §§ 484 and 496;

g. Violating the common law right of privacy via intrusion upon seclusion and publication of private facts;

h. Violating the Art. 1, § 1 of the California Constitution Right to Privacy;

i. Violating express contract promises to consumers;

j. Violating the duty of good faith and fair dealing; and

k. Violating the duty to hold Account Holders' personal information in confidence.

278. Google's conduct violated the spirit and letter of these laws, which protect property, economic and privacy interests, and prohibit unauthorized disclosure and collection of private communications and personal information.

279. Google stated it would not sell or disseminate Plaintiffs' and Class Members' personal information without their consent to other companies, except in limited situations not applicable here.

280. Google's conduct was immoral, unethical, oppressive, unscrupulous, and substantially injurious to Plaintiffs and Class Members. Further, Google's conduct narrowly benefitted its own business interests at the expense of Plaintiffs' and Class Members' fundamental privacy interests protected by the California Constitution and the common law.

281. Plaintiffs' and Class Members' loss of their personal information constitutes an economic injury.

282. Plaintiffs and Class Members have suffered harm in the form of lost property value, specifically the diminution of the value of their private and personally identifiable data and content.

283. Google's actions caused damage to and loss of Plaintiffs' and Class Members' property right to control the dissemination and use of their personal information and communications.

284. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including restitution, declaratory relief, reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5, injunctive relief, and all other equitable relief the Court determines is warranted.

COUNT FOUR: CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY

285. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

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

287. The phrase "and privacy" was added by an initiative adopted by California voters on November 7, 1972 (the Privacy Initiative).

288. The Privacy Initiative created a private right of action against nongovernmental entities for invasions of privacy.

289. The California Supreme Court has explained that, one of the principal "mischiefs" to which the Privacy Initiative was directed was "the overbroad collection and retention of unnecessary personal information by government and business interests." *White v. Davis*, 13 Cal.3d 757, 775 (Cal. 1975). "The moving force behind the new constitutional provision … relat[ed] to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society. The new provision's primary purpose is to

afford individuals some measure of protection against this most modern threat to personal privacy." *Id.* at 774.

290. The ballot language for the Privacy Initiative explained:

> Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American. … The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.
>
> *Fundamental to our privacy is the ability to control circulation of personal information*. This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often, we do not know that these records even exist and we are certainly unable to determine who has access to them.

White v. Davis, 13 Cal.3d at 774-75 (emphasis in original) (quoting ballot language).

291. Google's conduct in selling and sharing Plaintiffs' and Class Members' personal information in violation of its express unequivocal promises to the contrary is exactly why California voters adopted the Privacy Initiative in 1972.

292. Google creates "cradle-to-grave profiles" and detailed dossiers of Plaintiffs and Class Members, and then sells and shares the personal information contained in those profiles and dossiers with hundreds of different companies to aid those other companies for the purpose of making money and assisting those other companies in supplementing or building their own separate profiles and dossiers about Plaintiffs and Class Members.

293. As described herein, Google has intruded upon the following legally protected privacy interests of Plaintiffs and Class Members:

a. The right to privacy contained on personal computing devices, including web-browsing history;

b. The right to restrain business interests from misusing information gathered for one purpose in order to serve other purposes;

c. The right to control circulation of their personal information;

d. Statutory rights codified in federal and California privacy statutes;

e. The California Computer Crime Law, Cal Pen. Code § 502, which applies to all plaintiffs in this case by virtue of Google's choice of California law to govern its relationship with Google users;

294. Through the Terms of Service, other policies and other public statements set forth above, Google promised not to share or sell Plaintiffs' and Class Members' personal information without authorization.

295. Plaintiffs and Class Members had a reasonable expectation of privacy in the circumstances in that:

a. Plaintiffs and Class Members could not reasonably expect Google would commit acts in violation of federal and state laws as set forth below.

b. Google affirmatively promised users it would not share or sell their personal information without authorization.

296. Google's actions constituted a serious invasion of privacy in that it:

a. Violated several federal criminal laws, including the Electronic Communications Privacy Act.

b. Violated dozens of state criminal laws.

c. Invaded the privacy rights of hundreds of millions of Account Holders without their consent.

d. Disclosed sensitive personal information every time it shared information related to the verticals above relating to health, religion, ethnicity, race, or sexuality.

e. Enabled the targeting of Account Holders by third parties who did not have legal access to their personal information.

297. The surreptitious and unauthorized sharing and sale of the internet communications and associated personal information of millions of Account Holders constitutes an egregious breach of social norms.

298. Google lacked a legitimate business interest in sharing and selling Plaintiffs' and Class Members' personal information without their authorization.

299. In violating Plaintiffs' and Class Members' privacy in the manner described above, Google acted with oppression, fraud, or malice.

300. Plaintiffs and Class Members have been damaged by Google's invasion of their privacy and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

COUNT FIVE: INTRUSION UPON SECLUSION

301. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

302. A claim for intrusion upon seclusion requires (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

303. In carrying out its scheme to share and sell Plaintiffs' and Class Members' personal information without their consent, Google intentionally intruded upon the Plaintiffs' and Class Members' solitude or seclusion in that it effectively placed itself in the middle of Plaintiffs' and Class Members' communications to which it was not an authorized party and used data that they had not authorized Google to sell or share, but which it sold and shared anyway.

304. By engaging in cookie-matching with hundreds of other companies, Google intentionally intruded upon the Plaintiffs' and Class Members' solitude or seclusion. Cookie matching enabled companies with limited information about Plaintiffs and other Class Members to accumulate substantially more information about each individual Plaintiff and Class Member from Google.

305. By selling and sharing Plaintiffs' and Class Members' sensitive personal information for purposes of targeted advertising, Google intentionally intruded upon the Plaintiffs' and Class Members' solitude or seclusion in that it subjected Plaintiffs and Class Members to advertisements targeted to that sensitive information and publicized sensitive information to hundreds of other companies. Indeed, once sensitive information from Google account holders had been shared with other companies, there existed no way for account holders to further limit the continued spread of such information.

306. Google's actions were not authorized by the Plaintiffs and Class Members.

307. Google's intentional intrusion into Plaintiffs' and Class Members personal information, Internet communications, and computing devices was highly offensive to a reasonable

person in that Google violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

308. Google's unauthorized sharing and sale of personal information from hundreds of millions of Americans, including highly sensitive information about individuals' race, ethnicity, religion, health, and financial status, is highly offensive behavior.

309. Google's secret monitoring of web browsing for purposes of selling and sharing it with hundreds of unknown companies without Account Holders' consent is highly offensive behavior.

310. In intruding on Plaintiffs' and Class Members' seclusion in the manner described herein, Google acted with oppression, fraud, or malice.

311. Plaintiffs and Class Members have been damaged by Google's intrusion upon their seclusion and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

COUNT SIX: PUBLICATION OF PRIVATE INFORMATION

312. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

313. Plaintiffs' and Class Members' personal information, including their Internet communications and sensitive data, are private facts that Google promised not to share or sell to advertisers.

314. Google gave publicity to Plaintiffs' and Class Members' private facts and the content of their Internet communications by sharing and selling them to hundreds of different companies. Many of those companies have business models predicated on building massive databases of individual consumer profiles from which to sell targeted advertising and make further disseminations.

315. Plaintiffs and Class Members had no knowledge that Google was sharing and selling their personal information and did not authorize or consent to such publication.

316. Google's selling and sharing of patient personal information to hundreds of different advertising companies would be highly offensive to a reasonable person.

317. In disseminating Plaintiffs' and Class Members' personal information without their consent in the manner described above, Google acted with oppression, fraud, or malice.

318. Plaintiffs and Class Members have been damaged by the publication of their private information and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

COUNT SEVEN: BREACH OF CONFIDENCE

319. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

320. Plaintiffs and Class Members entrusted their personal information to Google.

321. The totality of Plaintiffs' and Class Members' personal information, including the content of their Internet communications, is confidential and novel.

322. Google knew that Plaintiffs' and Class Members' personal information was disclosed to Google in confidence. Indeed, Google's express promises to Plaintiffs and Class Members reflects its knowledge that their personal information was disclosed in confidence. Google told Account Holders:

a. "[W]hen you use our products, you trust us with your personal information. That's why we never sell your personal information." Ex. 5 at 1.

b. "When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information[.]" *E.g.*, Ex. 1 at 1; Ex. 15 at 1; Ex. 20 at 1.

323. As Google's CEO stated, "billions of people have trusted Google with questions they wouldn't have asked their closest friends." Ex. 25 at 1.

324. Google's CEO also stated, "To make privacy real, we give you clear, meaningful choices around your data. All while staying true to two unequivocal policies: that Google will never sell any personal information to third parties; and that you get to decide how your information is used." *Id.*

325. Google created and assumed a duty to protect Plaintiffs' and Class Members' confidential personal information by creating a legal relationship with them via its Terms of Service.

326. There was an understanding between Google on the one hand, and Plaintiffs and Class Members on the other, that Google would not betray their confidence by sharing their personal information without consent.

327. By disclosing and using Account Holders' personal information in violation of this understanding, Google breached the trust and confidence that Plaintiffs and Class Members placed in it.

328. In breaching Plaintiffs' and Class Members' confidence in the manner described above, Google acted with oppression, fraud, or malice.

329. Plaintiffs and Class Members have been damaged by Google's breach of trust and confidence and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

COUNT EIGHT: VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT

330. Google is subject to the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630-638. Google is headquartered in California; designed, contrived, and effectuated its practice of disclosing account holder information during the RTB process in California; and has adopted California substantive law to govern its relationship with Plaintiffs and all Class Members.

331. The California Invasion of Privacy Act states the following purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques 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.

332. Cal. Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner ….willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to 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 who uses, or attempts to use, in any manner, or for any purpose, or to

> communicate in any way, any information so obtained, or who 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, is punishable by a fine not exceeding two thousand five hundred dollars ….

333. Google is a "person" within the meaning of § 631(a).

334. By employing its Google RTB to sell and share Account Holder information to hundreds of Google RTB participants in real-time while communications between the Account Holders and first-party websites were still in transit or being sent or received within California, Google aided, agreed with, and conspired with Google RTB participants to aid them in reading, attempting to read, learning, or using the contents or meaning of the communications being exchanged connected to the Plaintiffs' and Class Members' personal information.

335. Plaintiffs and Class Members did not consent to Google's aid to or agreement with Google RTB participants in reading, attempting to read, learning, or using the contents or meaning of Plaintiffs' and Class Members' communications with websites that Plaintiffs and Class Members were directly interacting with.

336. The following items constitute "machine[s], instrument[s], or contrivance[s]" under § 631(a):

a. The cookies Google used to track, share, and sell the Plaintiffs' and Class Members' communications to Google RTB participants;

b. The Plaintiffs' and Class Members' browsers;

c. The Plaintiffs' and Class Members' personal computing devices;

d. Google's web servers;

e. The web servers of non-Google websites from which Google tracked, intercepted, shared, and sold the Plaintiffs' and Class Members' communications; and

f. The web servers of the Google RTB participants to which Google sold and shared Plaintiffs' and Class Members' communications; and

g. The computer code Google deployed to effectuate its scheme, including but not limited to Bid Requests for each Target Google caused to be submitted to Google RTB participants.

337. Even if the above-listed items do not constitute "machine[s], instrument[s], or contrivance[s]," Google's deliberate and purposeful efforts to facilitate its conduct comprise "any other manner."

338. Google's aid to the Google RTB participants occurred in "real time," as acknowledged by Google in its naming of the Google *Real-Time* Bidding system. As such, Google's aid to Google RTB participants occurred while Plaintiffs' and Class Members' communications with first-party websites were in transit or in the process of being sent or received.

339. Google's RTB documentation acknowledges that the information Google aided RTB participants in reading, attempting to read, or to learn included the "contents" and "meaning" of the Plaintiffs' and Class Members' communications with first-party websites. The "contents" or "meaning" re-directed within Google RTB Bid Requests include:

COMMUNICATIONS CONTENT	
cat	Array of IAB content categories of the site or app.
sectioncat	Array of IAB content categories that describe current section of site or app.
pagecat	Array of IAB content categories that describe current site or app page or view.
page	URL of the page where the impression will be shown.
ref	Referrer URL that caused navigation to the current page.
publisher	Details about the Publisher object of the site or app.
content	Details about the Content within the site or app.
keywords	Comma-separated list of keywords about this site or app.
content id	ID uniquely identifying the content.
episode	Content episode number (typically applies to video content).
title	Content title. Video examples: "Search Committee" (television); "A New Hope (movie); or "Endgame" (made for web). Non-video example: "Why an Antarctic Glacier is Melting So Quickly" (Time magazine article).
series	Content series. Video examples: "The Office" (television); "Star Wars" (movie); or "Arby 'N' The Chief (made for web). Non-video example: ("Ecocentric") (Time magazine blog).

"INFORMATION THAT WE KNOW ABOUT THE WEB PAGE OR MOBILE APP"		
17	Publisher ID	The publisher ID.
20	URL	The URL of the page with parameters removed.
VIDEO INFORMATION		
51	URL	The URL of the page that the publisher gives Google to describe the video content, with parameters removed.
61	Video title	The video title.
62	Video keywords	A list of keywords describing the video, extracted from the content management system of the video publisher.

340. Plaintiffs and Class Members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personal information.

341. Because Plaintiffs and Class Members have been injured by Google's violations of Cal. Pen. Code § 631, each seeks damages of the greater of $5,000 or three times the amount of actual damages, if any, sustained, as well as injunctive relief.

COUNT NINE: VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT – UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE

342. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

343. The Electronic Communications Privacy Act ("ECPA") prohibits the unauthorized interception of the content of any communication through the use of any device, and any subsequent disclosure or use of the intercepted contents of any electronic communication. 18 U.S.C. §2511.

344. ECPA protects both the sending and receipt of communications.

345. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

346. Google violated the interception provisions of the Electronic Communications Privacy Act ("ECPA") by:

a. Intentionally disclosing, or endeavoring to disclose, to other companies the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of electronic communications, in violation of 18 U.S.C. § 2511(1)(c); and/or

b. Intentionally using, or endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of electronic communications, in violation of 18 U.S.C. § 2511(1) (d).

347. ECPA defines interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

348. Google intercepted Plaintiffs' and Class Members' electronic communications, including the following content:

a. The precise text of GET and POST requests that Plaintiffs and Class Members exchanged with non-Google websites to which they navigated;

b. The precise text of Plaintiffs' and Class Members' search queries at non-Google websites to which they navigated and on which they entered such queries; and

c. Information that is a general summary or informs Google (and the Google RTB participants) of the subject of communications between Plaintiffs and Class members and the first-party websites.

349. Electronic Communications. The transmission of data between Plaintiffs and Class Members and the non-Google websites 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 or foreign commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

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

351. Google's developer documentation details the following content of electronic communications that it redirects to other companies in the Google RTB process:

COMMUNICATIONS CONTENT	
cat	Array of IAB content categories of the site or app.
sectioncat	Array of IAB content categories that describe current section of site or app.
pagecat	Array of IAB content categories that describe current site or app page or view.
page	URL of the page where the impression will be shown.
ref	Referrer URL that caused navigation to the current page.
publisher	Details about the Publisher object of the site or app.
content	Details about the Content within the site or app.
keywords	Comma-separated list of keywords about this site or app.
content id	ID uniquely identifying the content.
episode	Content episode number (typically applies to video content).
title	Content tile. Video examples: "Search Committee" (television); "A New Hope (movie); or "Endgame" (made for web). Non-video example: "Why an Antarctic Glacier is Melting So Quickly" (Time magazine article).
series	Content series. Video examples: "The Office" (television); "Star Wars" (movie); or "Arby 'N' The Chief (made for web). Non-video example: ("Ecocentric") (Time magazine blog).

"INFORMATION THAT WE KNOW ABOUT THE WEB PAGE OR MOBILE APP"		
17	Publisher ID	The publisher ID.
20	URL	The URL of the page with parameters removed.
VIDEO INFORMATION		
51	URL	The URL of the page that the publisher gives Google to describe the video content, with parameters removed.
61	Video title	The video title.

62	Video keywords	A list of keywords describing the video, extracted from the content management system of the video publisher.

352. Electronic, Mechanical, or Other Device. 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).

353. The following constitute devices within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Google used to acquire Plaintiffs' and Class Members' communications, including cookies Google sets, acquires, and discloses or sells to other companies through cookie-sharing;

b. The Plaintiffs' and Class Members' browsers;

c. The Plaintiffs' and Class Members' computing devices;

d. Google's web servers;

e. The web servers of the first-party non-Google websites from which Google tracked and intercepted the Plaintiffs' and Class Members' communications; and

f. The computer code deployed by Google to effectuate its tracking and interception of Plaintiffs' and Class Members' communications for purposes of forwarding them to hundreds of Google RTB participants, without authorization, including but not limited to data contained in Bid Requests.

354. Unauthorized Purpose. Google intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the unauthorized purpose of disclosing and selling those contents to Google's RTB participants.

355. Plaintiffs and Class members did not authorize Google to acquire the content of their communications for purposes of sharing and selling the personal information contained therein. Indeed, Google expressly and repeatedly promised that it would not share or sell user personal information, including browsing history.

356. Google's interception of the contents of Plaintiffs' and Class Members' communications was contemporaneous with their exchange with the websites to which they directed their communications. As described above, the Google RTB process occurs in milliseconds while the communication is still being exchanged between Plaintiffs and Class Members and the website to which they directed their communications. That is why Google itself refers to the process

as "Real-Time Bidding." The signal sent out to Google RTB is sent simultaneously with the signal sent to the websites to which Plaintiffs' and Class Members' communications were directed.

357. Google is not a party to Plaintiffs' and Class Members' electronic communications exchanged with the non-Google websites to which Plaintiffs and Class Members directed their communications.

358. Google acquired the content of Plaintiffs' and Class members' electronic communications with the non-Google websites to which their communications were directed through the surreptitious duplication, forwarding, and re-direction of those communications to Google. After intercepting the communications without authorization, Google then disclosed, sold, and shared the contents of the intercepted communications to hundreds of Google RTB participants and used the contents of the intercepted communications in furtherance of the Google RTB auction sales system.

359. Exceptions Do Not Apply. The ECPA prohibition on unauthorized interception contains exceptions. The burden is on the party seeking the benefit of an exception to prove its existence. Therefore, Plaintiffs need not affirmatively plead the absence of any exception. Nevertheless, Plaintiffs plead that Google's interceptions do not qualify for any exceptions.

360. ECPA provides an ordinary course of busines exception for liability, under which the communications at issue are, by definition, not intercepted. 18 U.S.C. § 2510(5)(a)(ii). This exception is narrow and protects from liability only where an electronic service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication. Google's interception of the contents of Plaintiffs' and Class Members' communications with any non-Google website to which they directed their browser does not facilitate and is not incidental to that communication. Rather, Google's interception facilitates a separate, unrelated communication – the contemporaneous communication of Plaintiffs' and Class Members' personal information to Google RTB participants.

361. ECPA provides an exception where one party to the communications provides consent to the disclosure of the communications at issue. 18 U.S.C. § 2511(2)(2). As detailed above, Plaintiffs and Class Members did not provide consent to the disclosure of the content of

their communications with Google RTB participants. To the contrary, Google promised in its Terms of Service and numerous other communications that it would not sell or share Account Holders' personal information absent their consent. Plaintiffs and Class Members were not asked for, and did not provide, such consent. Nor did Google procure the "lawful consent" of the websites to which Plaintiffs and Class Members directed and exchanged communications.

362. Similarly, the agreements that Google enters with publishers using Google's RTB process to fill ad space echo the promises Google makes to Account Holders. Google promises the website publishers that fill advertising space through Google RTB that Google's use of information will be "in accordance with Google's privacy policy" – the same privacy policy detailed above that expressly promises not to sell or share Account Holder information. Publishers who sign up for Google RTB must do so through the Google Ad Manager. At the end of the initial sign-up process, the publisher is promised, "Google's use of your information will be in accordance with Google's privacy policy." The privacy policy referenced is the same Privacy Policy that pertains to Account Holders, promising, as set forth above, that Google will not share or sell Account Holder personal information.

363. Likewise, the Google API Terms of Service promise, "By using our APIs, Google may use submitted information in accordance with our privacy policy." Again, the privacy policy referenced is the same Privacy Policy that pertains to Account Holders, promising, as set forth above, that Google will not share or sell Account Holder personal information.

364. Moreover, ECPA also contains an exception to the exception for single party consent. Under 18 U.S.C. § 2511(2)(d), an interception is unlawful and actionable even "where one of the parties to the communication has given prior consent to such interception" if the communication was "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."

365. As alleged throughout, Google's redirection, sale, and sharing of Plaintiffs' and Class Members' personal information and the contents of their Internet communications had the requisite criminal or tortious purpose for Plaintiffs' and Class Members' claims for intrusion upon seclusion; publication of private facts; tortious violation of Art. I, sec. 1 of the California

Constitution; breach of confidence; violation of the California UCL, Cal. Bus. & Prof. Code § 17200; the California Invasion of Privacy Act, Cal. Penal Code § 630; the California Computer Data Access and Fraud Act, Cal. Penal Code § 502; California Statutory Larceny, Cal. Penal Code §§ 484 and 496; the Electronic Communications Privacy Act, 18 U.S.C. §2511; and the Video Privacy Protection Act, 18 U.S.C. § 2710.

366. For the violations set forth above, Plaintiffs and Class Members seek appropriate preliminary and other equitable or declaratory relief; the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred. 18 U.S.C § 2520.

COUNT TEN: VIOLATION OF THE ECPA WIRETAP ACT – UNAUTHORIZED DISCLOSURE OF ELECTRONIC COMMUNICATIONS BY AN ECS

Subclass: All Google Account Holders Who Use the Google Chrome Browser

367. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

368. Plaintiffs are Account Holders who also use the Google Chrome web browser.

369. This count is brought on behalf of a subclass of all Google Account Holders who use the Google Chrome web browser.

370. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

371. Electronic Communication Service. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

372. The Google Chrome web browser is an electronic communication service. It provides to users thereof the ability to send or receive electronic communications. In the absence of a web browser or some other such system, Internet users could not send or receive communications over the Internet.

373. Intentional Divulgence. Google intentionally designed the Chrome web browser so that it would divulge the contents of Plaintiffs' and Subclass Members' communications with non-Google websites to hundreds of Google RTB participants.

374. While in Transmission. Google Chrome's divulgence of the contents of Plaintiffs' and Class Members' communications was contemporaneous with their exchange with the websites to which they directed their communications. As described above, the Google RTB process occurs in milliseconds while the communication is still being exchanged between Plaintiffs and Class Members and the websites to which they directed their communications. That is why Google itself refers to the process as "Real-Time Bidding." The signal sent out to Google RTB is sent simultaneously with the signal sent to the websites to which Plaintiffs' and Class Members' communications were directed.

375. Google Chrome is not a party to Plaintiffs' and Class Members' electronic communications exchanged with the non-Google websites to which Plaintiffs and Class Members directed their communications.

376. Google Chrome divulged the contents of Plaintiffs' and Class members' electronic communications with the non-Google websites to which their communications were directed through the surreptitious duplication, forwarding, and re-direction of those communications to Google. The divulgence of the contents of Plaintiffs' and Class Members' communications was without authorization. Google Chrome divulged the contents of Plaintiffs' and Class Members' communications to hundreds of Google RTB participants, entities other than the intended recipient of such communication, while Plaintiffs' and Class Members' communications were being transmitted on Google Chrome.

377. Exceptions Do Not Apply. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication":

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

18 U.S.C. § 2511(3)(b).

378. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

379. Google's divulgence of the contents of Plaintiffs' and Class Members' communications on the Chrome browser to hundreds of Google RTB participants was not authorized by 18 U.S.C. § 2511(2)(a) in that it was neither a necessary incident to the rendition of the Chrome service nor necessary to the protection of the rights or property of Google.

380. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

381. Google's divulgences of the contents of Plaintiffs' and Class Members' communications on the Chrome browser to hundreds of Google RTB participants was not done "with the lawful consent of the originator or any addressee or intended recipient of such communication[s]." As alleged above, Plaintiffs and Class Members, including members of the Subclass, did not authorize Google to divulge the contents of their communications to hundreds of Google RTB participants. Nor did Google procure the "lawful consent" of the websites to which Plaintiffs and Subclass Members directed and exchanged communications.

382. The other companies to which Google sold, shared, and divulged Plaintiffs' and Subclass Members' content of communications were not "person[s] employed or authorized, or whose facilities are used, to forward such communication[s] to [their] destination."

383. The contents of Plaintiffs' and the Subclass Members' communications did not appear to pertain to the commission of a crime, and Google Chrome did not divulge the contents of their communications to a law enforcement agency.

384. Plaintiffs and the Subclass Members seek appropriate preliminary and other equitable or declaratory relief; the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred. 18 U.S.C. § 2520.

COUNT ELEVEN: VIOLATION OF THE ECPA STORED COMMUNICATIONS ACT – UNAUTHORIZED DISCLOSURE OF ELECTRONIC COMMUNICATIONS BY AN ECS

On Behalf of a Subclass Comprising All Google Account Holders Who Use Google Chrome

385. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

386. This count is brought on behalf of a subclass of all Google Account Holders who use the Google Chrome web browser.

387. The ECPA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

388. Electronic Communication Service. ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

389. The Google Chrome browser is an ECS.

390. Electronic Storage. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

391. Google stores Plaintiffs' and Subclass Members' personal information and the contents of their communications in the Chrome browser and files associated with it.

392. Specifically, Google stores the content of Plaintiffs' and Subclass Members' Internet communications within the Chrome browser in two ways:

a. For purposes of backup protection so that if the browser inadvertently shuts down, Plaintiffs' and Subclass Members' can be presented with the option to restore their previous communications; and

b. For a temporary and intermediate amount of time incidental to the electronic transmission thereof when it places the contents of user communications into the browser's web-browsing history, which is only kept on the browser for 90 days.

393. When a Google Account Holder clicks a button or hits ENTER to exchange a communication with the website the Account Holder is interacting with while using the Chrome browser, the content of the communication is immediately placed into storage within the Chrome browser.

394. Google knowingly divulges the contents of Plaintiffs' and Subclass' members communications to hundreds of different companies through the Google RTB process while such communications are in electronic storage.

395. Exceptions Do Not Apply. Section 2702(b) of the Stored Communications Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;"

b. "as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service":

f. "to the National Center for Missing and Exploited Children, in connection with a reported submitted thereto under section 2258A;"

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency;" or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523."

396. The hundreds of other companies to which Google divulges the content of Plaintiffs' and Subclass Members' communications while stored in Chrome are not "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of the Plaintiffs' and Subclass members' communications.

397. Sections 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

398. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

399. Google's divulgence of the contents of user communications on the Chrome browser to hundreds of other companies through the Google RTB process was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither:

a. A necessary incident to the rendition of the Chrome service; nor

b. Necessary to the protection of the rights or property of Google.

400. Google's divulgence of the contents of user communications on the Chrome browser through the Google RTB process was not done "with the lawful consent of the originator or any addressee or intended recipient of such communication[s]."

401. As alleged above:

a. Plaintiffs and Google Account Holders, including members of the Subclass, did not authorize Google to divulge the contents of their communications to hundreds of other companies.

b. Google did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Subclass Members' were exchanging communications.

402. The hundreds of other companies to which Google divulges the content of Plaintiffs' and Subclass Members' communications while in Chrome storage through the RTB process are not "person[s] employed or whose facilities are used to forward such communication to its destination."

403. Google's divulgences in the RTB system were not to governmental entities.

404. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT TWELVE: VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT

On Behalf of a Subclass Comprising All Google Account Holders Who Use Google Chrome, Android Operating System, or Apps that Incorporate the Google Software Development Kit (SDK)

405. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

406. The Video Privacy Protection Act, 18 U.S.C. § 2710 ("VPPA") provides that "a video tape service provider" shall not "knowingly disclose[], to any person, personally identifiable information concerning any consumer of such provider" without informed written consent and not incident to the ordinary course of business. 18 U.S.C. § 2710(b)(1).

407. Video Tape Service Provider. Under the VPPA, a "video tape service provider" ("VTSP") is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection

(b)(2), but only with respect to the information contained in the disclosure." Under subparagraph (E) of subsection (b)(2), a VTSP is extended to include any person who obtains information "incident to the ordinary course of business of" the VTSP. As used in the VPPA, "'ordinary course of business' means only debt collection activities, order fulfillment, request processing, and transfer of ownership."

408. Google is a VTSP through its Chrome browser, Android operating system, and Google SDK that it provides to app developers:

a. Google Chrome, which establishes a supporting ecosystem to seamlessly deliver video content to consumers, is engaged in the delivery of audio visual materials similar to prerecorded video cassette tapes by providing software through which audio visual materials are requested or obtained by Plaintiffs and Subclass Members from various first-party websites accessed via the Chrome browser.

b. Google Android, which establishes a supporting ecosystem to seamlessly deliver video content to consumers, is engaged in the delivery of audio visual materials similar to prerecorded video cassette tapes by providing software through which audio visual materials are requested or obtained by Plaintiffs and Subclass Members at various first-party websites accessed via a mobile device running the Android operating system.

c. The Google SDK, which establishes a supporting ecosystem to seamlessly enable companies such as ESPN and Brid.tv, a provider of enterprise solutions for managing and monetizing customers' video that is also a Google Ad Manager certified external vendor, to deliver video content to consumers, is engaged in the delivery of audio visual materials similar to prerecorded video cassette tapes by providing software through which audio visual materials are requested or obtained by Plaintiffs and Subclass Members at various first-party websites that make use of the Google SDK to provide such audio visual materials.

d. Google Chrome, Android, and the Google SDK each also qualify as VTSPs through 18 U.S.C. § 2710(b)(2)(E) because they are Google services that aid VTSPs in order fulfillment and request processing.

409. Personally Identifiable Information. Under the VPPA, "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a" VTSP. 18 U.S.C. § 2710(a)(3).

410. The VPPA definition of "personally identifiable information" is purposefully broad and open-ended. The VPPA "prohibits … [the disclosure of] 'personally identifiable information' – information that links the customer or patron to particular materials or services." S. Rep. No. 100-

599 at *7. "Unlike the other definitions [in the VPPA], paragraph (a)(3) uses the word 'includes' to establish a minimum, but not exclusive, definition of personally identifiable information." S. Rep. No. 100-599 at *12. The Act was passed in 1988 following publication of "a profile of Judge Robert H. Bork based on the titles of 146 files *his family had rented* from a video store." S. Rep. 100-599 at 6 (emphasis added).

411. Google knowingly discloses personally identifiable information about Plaintiffs' and Subclass Members' requests, acquisitions, and viewing records of specific video materials and services.

412. The Google RTB developer documentation for Bid Requests states that it discloses the following information about Plaintiffs and Subclass Members to hundreds of different companies, including regarding the audio-visual materials they access through Google Chrome, Android, and Google SDK:

COMMUNICATIONS CONTENT	
cat	Array of IAB content categories of the site or app.
sectioncat	Array of IAB content categories that describe current section of site or app.
pagecat	Array of IAB content categories that describe current site or app page or view.
page	URL of the page where the impression will be shown.
ref	Referrer URL that caused navigation to the current page.
publisher	Details about the Publisher object of the site or app.
content	Details about the Content within the site or app.
keywords	Comma-separated list of keywords about this site or app.
content id	ID uniquely identifying the content.
episode	Content episode number (typically applies to video content).
title	Content title. Video examples: "Search Committee" (television); "A New Hope (movie); or "Endgame" (made for web). Non-video example: "Why an Antarctic Glacier is Melting So Quickly" (Time magazine article).
series	Content series. Video examples: "The Office" (television); "Star Wars" (movie); or "Arby 'N' The Chief (made for web). Non-video example: ("Ecocentric") (Time magazine blog).
DEVICE	
dnt	Standard 'Do Not Track' flag as set in the header by the browser.
ua	Browser user-agent string.
ip	IPv4 address closest to device.
geo	Location of the device assumed to be the user's current location defined by a Geo object.
didsha1	Hardwire device ID.
dpidsha1	Platform device ID (e.g. Android ID).
ipv6	IPv6 address closest to device.
carrier	Carrier or ISP, using exchange curated string names which should be published to bidders a priori.
make	Device make (e.g. Apple).
model	Device model (e.g. iPhone).

os	Device operating system (e.g. iOS).
osv	Device operating system version.
hwv	Hardware version of the device (e.g. '5S' for iPhone 5S).
devicetype	The general type of device.
ifa	ID sanctioned for advertiser use in the clear.
macsha1	MAC address of the device.
GEO-LOCATION	
lat	Latitude from -90.0 to 90.0, where negative is south.
lon	Longitude from -180.0 to 180.0 where negative is west.
country	Country.
region	Region.
metro	Google metro code; similar to but not exactly Nielson DMAs.
city	City using United Nations Code for Trade & Transport.
zip	Zip/postal code.
type	Source of location data.
accuracy	Estimated location accuracy.
lastfix	Number of seconds since this geolocation fix was established.
USER	
Id	Exchange-specific id for the user.
Buyerid	Buyer-specific ID as mapped by the exchange for the buyer.
Gender	Gender as 'M' male, 'F' female, 'O' other.
Keywords	Comma-separated list of keywords, interests, or intent.
Customdata	Optional feature to pass bidder data set in the exchange's cookie.
Geo	Location of the user's home based defined by a Geo object. This is not necessarily their current location.
Data	Values for this field are now redacted. Segment.id references the exchange-detected vertical of the page. Segment.value corresponds to the weight of that detected vertical, a higher weight suggesting the page is more relevant for the detected vertical.

"INFORMATION THAT WE KNOW ABOUT THE USER"		
2	IP address	The first 3 bytes of IPv4 or first 6 bytes for IPv6.
3	Special Treatment	Reasons for special treatment of user data. For example, if the "current request should be treated as child-directed for purposes of the Children's Online Privacy Protection Act."
4	Google ID	"The Google ID for the user. … This field may be the same as the Google ID returned by the cookie matching service."
5	Google ID Version	"The version number of the google_user_id. We may sometimes change the mapping from cookie to google_user_id."
6	Google ID Age	"The time in seconds since the google_user_id was created."
7	Match Data	"Match data stored for this google_user_id through the cookie matching service. If a match exists, then this field holds the decoded data that was passed in the google_hm parameter."
8	User-Agent	"A string that identifies the browser and type of device that sent the request."
9	FLoC	"The value of a cohort ID – a string identifier that is common to a large cohort of users with similar browsing habits. … Experimental feature: may be subject to change."
10	User Agent Info.	"This will be populated with information about the user agent, extracted from the User-Agent header."
11	Publisher location	The billing address country of the publisher.
12	End-user location	The user's approximate geographic location.
13	Zip code	Detected postal code of the user.

14	Hyper-local	A hyperlocal targeting location when available.
15	User verticals	"List of detected user verticals. Currently unused. This field is not populated by default. We recommend that bidders instead store and look up list ids using either google_user_id or hosted-match-data as keys."
16	User-list	The user list id.
INFORMATION FOR "AD QUERIES COMING FROM MOBILE DEVICES"		
41	Mobile App	The identifier of the mobile app or mobile webpage. "If the app was downloaded from the Apple iTunes app store, then this is the app-store id, e.g. 343200656. For Android devices, this is the fully qualified package name, e.g. com.rovio.angrybirds. For Windows devices, it's the App ID, e.g. f15abcde-f6gh-47i0-j3k8-37193817mn3o. For SDK-less requests (mostly from connected TVs), the app ID provided by the publisher directly in the request."
45	Advertising IDs	This field is used for advertising identifiers for: 1) iOS devices (This is called Identifier for Advertising or IDFA, as described at https://support.google.com/authorizedbuyers/answer/3221407) 2) Android devices; 3) Roku devices; 4) Microsoft Xbox devices; 5) Amazon devices (i.e. Amazon Fire)
46	App Name	App names for Android by Google Play and for iOS by App Annie.
VIDEO INFORMATION		
50	Placement	Where the ad is placed.
51	URL	The URL of the page that the publisher gives Google to describe the video content, with parameters removed.
52	Playback Method	How the video ad will be played.
53	Clickable	Describes whether the video ad is clickable.
54	Start-Delay	The time in milliseconds from the start of the video when the ad will be displayed.
55	Ad Duration	The minimum and maximum ad durations.
56	Skippable	Whether the publisher allows users to skip the ad.
57	Protocols	Supported video protocols.
58	File formats	Supported video file formats.
59	Companion Ads	Information about companion ad slots shown with the video.
60	Size	Height and width for the video ad.
61	Video title	The video title.
62	Video keywords	A list of keywords describing the video, extracted from the content management system of the video publisher.

413. Many of the companies to which Google knowingly discloses Plaintiffs' and Class Members' video purchases and viewing habits already maintain their own databases of identifiers for Plaintiffs and Class Members. For example, Google and Facebook have reached a deal worth at least $500 million annually associated with Facebook's use of Google RTB. Google knows that Google Chrome, Android, and Google SDK provide enough personally identifying information to Facebook to allow it to identify the individual Account Holder. Other companies to which Google discloses Plaintiffs' and Class Members' video purchases and viewing habits are able to identify

the individual Account Holder because Google provides a cookie-match system that it knows enables them to match the disclosed Google IDs to their own proprietary IDs for Plaintiffs and Class Members.

414. In addition, the identifiers Google discloses to the Google RTB participants are readily capable of being used by those companies to identify specific users even in the absence of a pre-existing database possessed by the recipient of Google's disclosures. For example, *The New York Times* investigation detailed above used the same type of data disclosed on Google RTB to identify specific people who participated in the assault on the United States Capitol on January 6, 2021.

415. Exceptions Do Not Apply. Certain types of disclosures are permitted under the VPPA. Establishing the existence of such circumstances is an affirmative defense. Regardless, none exists here.

416. Google did not receive sufficient informed, written consent from Plaintiffs and Class Members to permit disclosure. 18 U.S.C. § 2710(b)(2)(B).

417. Disclosure was not made to law enforcement pursuant to a warrant, grand jury subpoena, or court order. 18 U.S.C. § 2710(b)(2)(C); *see* 18 U.S.C. § 2710(b)(2)(F) (permitting disclosure pursuant to a court order, in a civil proceeding, upon a showing of compelling need for the information that cannot be accommodated by other means, where the consumer is given reasonable notice of the court proceeding and afforded the opportunity to appear and contest the claim of the person seeking disclosure).

418. Disclosure was not solely of the names and addresses of Plaintiffs and Class Members where they were provided a clear and conspicuous opportunity to prohibit the disclosure and the disclosure did not disclose the title, description, or subject matter of any audio visual material. 18 U.S.C. § 2710(b)(2)(D).[75]

[75] While the subject matter may be disclosed for the exclusive use of marketing goods and services directly to the consumer, such disclosure remains conditioned on the consumer's clear and conspicuous opportunity to prohibit such disclosure. *Id.* That opportunity was not made available to Plaintiffs and Class Members here.

419. Disclosure was not incident to the ordinary course of business for Google Chrome, Android, or Google SDK. 18 U.S.C. § 2710(b)(2)(E).

420. For Google's VPPA violations, the Subclass who uses Google Chrome, the Android mobile operating system, or apps that incorporate the Google SDK seeks actual damages but no less than liquidated damages in an amount of $2,500; punitive damages; reasonable attorneys' fees and other litigation costs reasonably incurred; and such other preliminary and equitable relief as the court determines to be appropriate. 18 U.S.C. § 2710(c).

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award Plaintiffs and the Class the measure of unjust enrichment enjoyed by Defendant as a result of its violations identified herein, in an amount to be proven at trial, including interest thereon;

D. Award Plaintiffs and the Class punitive damages pursuant to Cal. Civ. Code § 3294(a), as Google acted with oppression, fraud, or malice;

E. Award Plaintiffs declaratory relief in the form of an order finding the following, along with all other forms of declaratory relief the Court finds appropriate:

a. Google breached the contractual rights of its users;

b. Google's actions violated the duty of good faith and fair dealing;

c. Google's actions violated California's Unfair Competition Law;

d. Google's actions violated Art. 1, § 1 of the California Constitution, Right to Privacy;

e. Google's actions constitute an intrusion upon seclusion;

f. Google's actions constitute publication of private information;

g. Google's actions violated the duty of confidence;

h. Google's actions violated California's Invasion of Privacy Act;

i. Google's actions violated the Electronic Communications Privacy Act;

j. Google's actions violated the Video Privacy Protection Act;

k. Plaintiffs have suffered privacy harm; and

l. Plaintiffs have suffered economic harm.

E. Permanently enjoin Google, its officers, agents, servants, employees, and attorneys, from sharing or selling any existing Google account holder's personal information without express authorization for the sale of such information;

D. Award Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

E. Grant Plaintiffs such further relief as the Court deems appropriate.

VIII. JURY TRIAL DEMAND

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

Dated: March 26, 2021

BLEICHMAR FONTI & AULD LLP

By: */s/ Lesley Weaver*

Lesley Weaver (Cal. Bar No. 191305)
Matthew S. Melamed (Cal. Bar No. 260272)
Anne K. Davis (Cal. Bar No. 267909)
Angelica M. Ornelas (Cal. Bar No. 285929)
Joshua D. Samra (Cal. Bar No. 313050)
555 12th Street, Suite 1600
Oakland, CA 94607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com
mmelamed@bfalaw.com
adavis@bfalaw.com
aornelas@bfalaw.com
jsamra@bfalaw.com

SIMMONS HANLY CONROY LLC

By: */s/ Jay Barnes*

Mitchell M. Breit (*pro hac vice* to be sought)

Jason 'Jay' Barnes (*pro hac vice* to be sought)
An Truong (*pro hac vice* to be sought)
Eric Johnson (*pro hac vice* to be sought)
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
Fax: (212) 213-5949
mbreit@simmonsfirm.com
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

PRITZKER LEVINE LLP

By: */s/ Elizabeth C. Pritzker*
Elizabeth C. Pritzker (Cal. Bar No. 146267)
Jonathan K. Levine (Cal Bar No. 220289)
Caroline C. Corbitt (Cal Bar No. 305492)
1900 Powell Street, Suite 450
Emeryville, CA 94608
Tel.: (415) 692-0772
Fax: (415) 366-6110
ecp@pritzkerlevine.com
jkl@pritzkerlevine.com
ccc@pritzkerlevine.com

Attorneys for Plaintiffs

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)

I, Lesley E. Weaver, attest that concurrence in the filing of this document has been obtained from the other signatories. I declare under penalty of perjury that the foregoing is true and correct.

Executed this 26th day of March, 2021, at Oakland, California.

/s/ Lesley Weaver
Lesley E. Weaver