

1 NANJI E. NISHIMURA (SBN 152621)
 nnishimura@cpmlegal.com
 2 BRIAN DANITZ (SBN 247403)
 bdanitz@cpmlegal.com
 3 KARIN B. SWOPE (Pro Hac Vice pending)
 kswope@cpmlegal.com
 4 NOORJAHAN RAHMAN (SBN 330572)
 nrahman@cpmlegal.com
 5 BETHANY M. HILL (SBN 326358)
 bhill@cpmlegal.com
 6 **COTCHETT, PITRE & MCCARTHY, LLP**
 840 Malcolm Road
 7 Burlingame, California 94010
 Telephone: (650) 697-6000
 8 Facsimile: (650) 697-0577

MAISIE C. SOKOLOVE (SBN 239665)
 mcs@knoxricksen.com
 THOMAS E. FRAYSSE (SBN 104436)
 tef@knoxricksen.com
 ITAK K. MORADI (SBN 310537)
 ikm@knoxricksen.com
KNOX RICKSEN LLP
 2033 N. Main St., Suite 340
 Walnut Creek, CA 94596
 Telephone: (925) 433-2500
 Facsimile: (925) 433-2505

Attorneys for Plaintiffs and the Class

10 **UNITED STATES DISTRICT COURT**
 11 **NORTHERN DISTRICT OF CALIFORNIA**
 12 **SAN JOSE DIVISION**

14 **MEAGHAN DELAHUNTY,**
MEGHAN CORNELIUS, and
 15 **JOHN KEVRANIAN, on behalf of**
 16 **themselves and all others similarly**
situated,

Plaintiffs

vs.

GOOGLE, LLC.,

Defendants.

CASE NO:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

	<u>Page</u>
I. INTRODUCTION	1
A. The Falsehood Presented by Google re Privacy	1
B. The Process of Google’s Privacy Violations	1
C. The Scale of Google’s Privacy Violations	3
D. Google’s Continuing False Promises Regarding Privacy	3
E. The Violations of both California and Federal Law	5
F. Congressional Inquiry has not Stopped the Fraud	6
II. JURISDICTION	7
III. PARTIES	8
IV. FACTS	10
G. Google Falsely Represents That It Protects Its Customers’ Privacy	10
H. Google’s History of Privacy Violations & Its Agreement with the Federal Trade Commission	12
I. Google Promises That It Doesn’t Sell Customers’ Personal Information	15
1. The Privacy Policy Provided Personal Information Was Not Shared or Sold	16
2. Terms of Service from May 2018 to the Present.....	18
J. Google Real-Time Bidding is Hidden to Google Customers	19
1. How Google Customers’ Personal Information is Shared on the RTB Auction	21
2. Google’s Disclosures Are Personally Identifiable to RTB Participants.....	22
3. Companies Buy and Google Sells Google Customers’ Personal Information	23
4. Statute of Limitations is Tolled	25
K. Google has been wrongly enriched by its conduct	25
L. Plaintiffs’ personal information is property under California law	26
M. The California Financial Privacy Act Imposes Information Fiduciary Obligations Upon Google	27
V. CLASS ACTION ALLEGATIONS	29
VI. CAUSES OF ACTION	31
FIRST CLAIM FOR RELIEF	
CALIFORNIA INVASION OF PRIVACY	31

1 **SECOND CLAIM FOR RELIEF**
2 BREACH OF IMPLIED CONTRACT 32

3 **THIRD CLAIM FOR RELIEF**
4 BREACH OF FIDUCIARY DUTY 33

5 **FOURTH CLAIM FOR RELIEF**
6 UNJUST ENRICHMENT 34

7 **FIFTH CLAIM FOR RELIEF**
8 VIOLATIONS OF THE CALIFORNIA UNFAIR
9 COMPETITION LAW (“UCL”)
10 Cal. Bus. & Prof. Code § 17200, *et seq.* 35

11 **SIXTH CLAIM FOR RELIEF**
12 INTRUSION UPON SECLUSION 36

13 **SEVENTH CLAIM FOR RELIEF**
14 PUBLICATION OF PRIVATE INFORMATION 37

15 **EIGHTH CLAIM FOR RELIEF**
16 BREACH OF CONFIDENCE 38

17 **NINTH CLAIM FOR RELIEF**
18 VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT 39

19 **TENTH CLAIM FOR RELIEF**
20 VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT –
21 UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE 41

22 **ELEVENTH CLAIM FOR RELIEF**
23 VIOLATION OF ECPA WIRETAP AND STORED COMMUNICATIONS ACT –
24 UNAUTHORIZED DISCLOSURE OF ELECTRONIC COMMUNICATIONS..... 44

25 **TWELTH CLAIM FOR RELIEF**
26 VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT 49

27 **THIRTEENTH CLAIM FOR RELIEF**
28 BREACH OF CONTRACT 52

29 **FOURTEENTH CLAIM FOR RELIEF**
30 BREACH OF THE IMPELIED COVENANT OF
31 GOOD FAITH AND FAIR DEALING 53

32 **FIFTEENTH CAUSE OF ACTION**
33 STATUTORY CIVIL LARCENY
34 California Penal Code Sections 484 and 496 54

35 **VII. JURY TRIAL DEMAND..... 56**

1 **“Few Americans realize that some auction participants are siphoning off and storing**
2 **“bidstream” data to compile exhaustive dossiers about them. In turn, these dossiers**
3 **are being openly sold to anyone with a credit card, including to hedge funds,**
4 **political campaigns, and even to governments.”**

5 *April 1, 2021 Letter to Google CEO Sundar Pichai from*
6 *U.S. Senators Wyden, Cassidy, Gillibrand, Warner, Brown, and Warren*¹

7 **I. INTRODUCTION**²

8 **A. The Falsehood Presented by Google re Privacy**

9 1. This case is all about a persons’ privacy under laws of our state, country and
10 common sense.

11 2. Google repeatedly says that it values privacy and gives users control of their
12 personal information. Google promises its hundreds of millions of users that it **“will never sell**
13 **any personal information to third parties”** and **“you get to decide how your information is**
14 **used.”**³ These promises are false. In fact, Google monitors its consumers’ digital footprint, then
15 makes billions of dollars by selling their sensitive personal information. While Google lulls its
16 users into a false sense of privacy, it continually and surreptitiously broadcasts its users’
17 sensitive personal information to third parties through its Real-Time Bidding (“RTB”) system.

18 **B. The Process of Google’s Privacy Violations**

19 3. RTB is the process by which the digital ads we see every day on the Internet are
20 curated. For each ad, an auction takes place milliseconds before it shows up in a users’ browser
21 or in an mobile application. During this auction, hundreds of third parties receive sensitive
22

23 _____
24 ¹ See Exhibit 1 to this Complaint.

25 ² Plaintiffs bring this action on behalf of themselves and all others similarly situated. The
26 allegations pertaining to plaintiffs are based on personal knowledge, and the allegations
27 pertaining to all other matters are based on information and belief, including investigations by
28 counsel and information learned from Congressional hearings, administrative proceedings,
academic research, Google’s website, and news reports.

³ 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/opinion/google-sundar-pichai-privacy.html>

1 personal information about the potential recipient of the ad, including, but not limited to, their
2 device identifiers and their cookies, detailed location data, IP addresses, browsing history, unique
3 demographic and biometric information such as age and gender. All of these “bidders” receive
4 this personal information which they can, and do, save and review, even though only one
5 bidder—the auction winner—will use that information to deliver an advertisement to the
6 consumer.

7 4. Few Americans realize that Google is allowing so many companies to siphon off
8 and store this highly personal “bidstream” data which is then sold by data brokers to hedge
9 funds, political campaigns, and even to governments, both foreign and domestic.⁴ When
10 compiled, these massive data sets operate like exhaustive dossiers on individual Americans.

11 5. During its Real-Time Bidding auctions, Google solicits participants to bid on ad
12 space targeted to the specific consumer (the “Consumer”). To do so, Google provides highly
13 specific information about the Consumer to all auction participants, including data that
14 effectively identifies the Consumer being targeted through unique identifiers, device identifiers
15 and IP addresses, among other information. All of this individualized information is called the
16 “Bidstream Data.”

17 6. In less than a blink of an eye, hundreds of recipients of the Consumer’s Bidstream
18 Data submit bids to place an ad on the Consumer’s screen. Only one bidder will win the auction.
19 However, all participants, even those who did not even submit a bid, are able to save, store and
20 monetize the Consumer’s personal information. As Google is well-aware, many participants do
21 not place bids and only participate to conduct surveillance and collect ever more detailed data
22 points about millions of Google’s Consumers. Google benefits from this surveillance, as the
23 higher number of bidders encourages higher bids, which increases the profitability of Google
24 RTB auctions.

25
26 _____
27 ⁴ Senator Ron Wyden (Oregon), et al. (July 31, 2020), Letter to Hon. Joseph J. Simmons,
28 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> and attached as Ex 1 to this Complaint

1 **C. The Scale of Google’s Privacy Violations**

2 7. Google’s RTB auction process is the most extensive in the world and the resulting
3 targeted advertising is **the primary source** of Google’s over **One Hundred and Fifty Billion**
4 **Dollars** (>\$150,000,000,000) in annual revenues. Google’s position as one of the world’s most
5 pervasive technology companies, has given it unique access to the intimate details of each
6 Consumer’s habits and preferences. Google’s extensive access to consumer data is facilitated by
7 its various (and often seemingly free) consumer products, including the ubiquitous Google.com
8 search engine, Google Maps, the Chrome web-browser, Gmail, YouTube, Android, Google
9 Documents, Google Drive, Google Calendars, Google Flights, Google Fit, Google Pay, etc.
10 Each of these products provides Google with an opportunity to gather detailed personal
11 information about its consumers as they engage online in real-time.

12 8. Google’s purpose is to build massive repositories of the most current information
13 available about the people using its services to sell it to Google’s partners. Google secretly
14 collects and analyzes real-time information about everyone engaging on those platforms and on
15 third-party platforms through services such as Google Analytics. This results in Google
16 collecting and selling information about activity users could not expect to be sold. But because
17 transparency about those practices would lead to less user engagement on those platforms, which
18 in turn would impede its ability to maximize targeted ad revenues, Google does not disclose
19 these practices to its account holders.

20 **D. Google’s Continuing False Promises Regarding Privacy**

21 9. This pervasive collection and use of its consumers’ personal information
22 contradicts Google’s promises of user privacy and control. Any consumer can sign up for a
23 Google Account by clicking a button assenting to the TOS Google has unilaterally drafted which
24 falsely promises consumers:

- 25 • **“We don’t sell your personal information to anyone.”⁵**
- 26 • **“We don’t share information that personally identifies you with**
- 27 **advertisers.”⁶**

28 _____
⁵ <https://about.google/how-our-business-works/>

- 1 • “Advertisers do not pay us for personal information.”⁷
- 2 • “We also never use ... sensitive information like race, religion, or
- 3 sexual orientation, to personalize ads to you.”⁸
- 4 • “We don’t show you personalized ads based on sensitive categories,
- 5 such as race, religion, sexual orientation, or health.”⁹
- 6 • “You get to decide how your information is used.”¹⁰



7
8
9
10 Your privacy is protected by
11 responsible data practices.
12

11

13
14 10. These representations are intentionally false. The Bidstream Data that Google
15 sells and discloses to all Google RTB auction participants includes the Google Customer’s
16 unique device identifier; his/her IP address and Google ID; his/her “User-Agent” information;
17 the content of the webpage the Google customer is viewing; the “Publisher ID of the website;
18 and so-called “vertical” information about the Google Customer’s interests that is associated
19 with the bid that can include information relating to race, religion, health, and sexual orientation.
20 The vertical information is collected by Google over time and organized for each and every
21
22

23
24 ⁶Google Privacy Policy dated Feb. 4, 2021.

25 ⁷ *Id.*

26 ⁸ <https://about.google/how-our-business-works/>

27 ⁹ Google Privacy Policy dated Feb. 4, 2021.

28 ¹⁰ 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/opinion/google-sundar-pichai-privacy.html>

¹¹ *Your privacy is protected by responsible data practices*, Google, https://safety.google/intl/en_us/privacy/data/ (last visited Apr. 24, 2021).

1 Google Customer by algorithm into thousands of consumer categories that identify the user's
2 personal habits, interests and preferences.

3 11. As a result, in the blink of an eye, millions of times a day, Google provides each
4 and every RTB auction participant with a wealth of information about Google Customers,
5 including the identity of the customer, their specific device, their specific location; the specific
6 content of their communications; and highly sensitive information about race, religion, sexual
7 orientation, and health.

8 12. Google even provides RTB bidders with a service that helps them match up the
9 Google Customer's current Bidstream Data with the library of information that the recipient has
10 already collected regarding that Google Customer.

11 13. The extensive and detailed nature of this personalized profile that is collected in
12 real-time by Google about each of its customers, over time, is why Google is able to charge
13 premium prices from Google RTB auction bidders for placing targeted ads related to each
14 Google Customer's activity on the Internet.

15 14. All participants in Google RTB auctions including those who do not actually
16 place bids, can save, store and use the Bidstream Data for each Google Customer. Once a Google
17 Customer's Bidstream Data is published by Google, the data is not recoverable.

18 **E. The Violations of both California and Federal Law**

19 15. Google adopts California law in its contract with Google Customers. The
20 Bidstream Data provided by Google constitutes personal information under California law and
21 the exchange of that data for participation in the auction constitutes a sale of that personal
22 information. Google's sale of its customers' personal information breaches its express promises
23 and violates laws that prohibit the selling of users' personal and highly sensitive information.

24 16. Google's RTB process is largely unseen and unknown to Google Customers.
25 Google does not disclose to its Google Customers its creation and use of massive data sets to
26 profile them in these auctions, and it does not have Google Customers' consent for such activity.
27 The Bidstream Data information that is exchanged every second of every day in Google's RTB
28 auctions are not identified in any of Google's voluminous public-facing policies and TOS. The

1 scale and success of Google’s RTB auction process is based on the fact that it is invisible to the
2 millions of Google Customers whose personal and sensitive information is bought and sold every
3 second of every day.

4 17. But for Google’s deceptive practices concerning its collection and use of its
5 customers’ personal information, users would have turned to other less-invasive options for
6 browsing the Internet, Google’s customer base would have decreased, and fewer bidders would
7 have participated in Google’s RTB auctions, which in turn would have decreased the massive
8 profits Google derives from its hidden RTB auctions.

9 18. Google’s blatant misdirection about user privacy is astonishing, but is part of
10 Google’s general culture of disregard for users’ privacy, and is consistent with Google’s
11 unscrupulous business practices.¹²

12 19. Google’s practices affect millions of Americans who care about protecting their
13 privacy. According to Google, more than 200 million people visit Google’s “Privacy Checkup”
14 website each year. Each day, nearly 20 million people check their Google privacy settings.
15 People do this because they care about their privacy and believe that they can “control” what
16 Google shares (because Google has told them so). The truth is that Google “controls” how it uses
17 consumer data, and its representations about consumer control are meaningless.

18 **F. Congressional Inquiry has not Stopped the Fraud**

19 20. This process has been the subject of Congressional inquiry. In July 2020, Senator
20 Ron Wyden and nine other members of Congress wrote a letter to the Federal Trade Commission
21 explaining the privacy dangers of RTB systems. The letter explained: **“Americans never agreed
22 to be tracked and have their sensitive information sold to anyone with a checkbook. ... This
23 outrageous privacy violation must be stopped and the companies that are trafficking in**

24
25
26 ¹² Nicholas Kristof, *With Help from Google, XVideos Lets People Leer at the Worst Moment in a*
27 *Child’s Life*, New York Times (April 16, 2021), available at
28 <https://www.nytimes.com/2021/04/16/opinion/sunday/companies-online-rape-videos.html>
(reporting on Google’s role in directing people to video footage of child sexual abuse: “Google is
the primary means by which [‘porn tubes’] drive traffic to their sites”).

1 **Americans’ illicitly obtained private data should be shut down.”¹³**

2 21. On April 1, 2021, a bipartisan group comprised of U.S. Senators Wyden, Cassidy,
3 Gillibrand, Warner, Brown, and Warren, sent letters to Google and other tech companies
4 engaged in buying and selling targeted ads through RTB, demanding answers to questions
5 concerning the continuous selling of personal consumer information to all comers, including
6 foreign governments:

7 **Few Americans realize that some auction participants are**
8 **siphoning off and storing “bidstream” data to compile**
9 **exhaustive dossiers about them. In turn, these dossiers are**
10 **being openly sold to anyone with a credit card, including to**
11 **hedge funds, political campaigns, and even to governments.**

12 **Over the past year, multiple reports have indicated that a**
13 **number of federal agencies have purchased personal data**
14 **derived from mobile apps and other online services, in ways**
15 **that potentially merit closer scrutiny. But the United States is**
16 **not the only government with the means and interest in**
17 **acquiring Americans’ personal data. This information would**
18 **be a goldmine for foreign intelligence services that could**
19 **exploit it to inform and supercharge hacking, blackmail, and**
20 **influence campaigns. As Congress debates potential federal**
21 **privacy legislation, we must understand the serious national**
22 **security risks posed by the unrestricted sale of Americans’**
23 **data to foreign companies and governments.¹⁴**

24 22. Plaintiffs bring this class action on behalf of themselves and all Google
25 Customers in the United States who, by virtue of browsing on the Chrome browser, was subject
26 to violations of privacy, and other violations of statutory, Constitutional and common law by
27 having their personal information sold or otherwise disclosed by Google without their
28 authorization.

29 **II. JURISDICTION**

30 23. This Court has subject matter jurisdiction over the federal claims in this action.

31 ¹³ See Exhibit 2 to this Complaint, Wyden FTC Letter.

32 ¹⁴ See April 1, 2021 letter to Sundar Pichai; Exhibit 1 to the Complaint, and available at
33 [https://www.wyden.senate.gov/imo/media/doc/040121%20Wyden%20led%20Bidstream%20Let
34 ter%20to%20Google.pdf](https://www.wyden.senate.gov/imo/media/doc/040121%20Wyden%20led%20Bidstream%20Letter%20to%20Google.pdf)

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

5 24. This Court has supplemental jurisdiction over the state law claims in this action
6 pursuant to 28 U.S.C. § 1367 because the state law claims arise out of the same case or
7 controversy as those that give rise to the federal claims.

8 25. This Court has personal jurisdiction over Defendant Google LLC (“Defendant” or
9 “Google”) because it is headquartered in this District. Google concedes to personal jurisdiction
10 in its current and prior Google TOS.¹⁵

11 26. This District is the correct venue because Google is headquartered in this District
12 and because its TOS provides that Plaintiffs resolve disputes in this District.

13 27. Assignment of this case to the San Jose Division is correct because a substantial
14 part of the events or omissions giving rise to Plaintiffs’ claims occurred in Santa Clara County,
15 California. *See* Civil Local Rule 3-2(c)(e)

16 **III. PARTIES**

17 28. Plaintiff Meaghan Delahunty is a citizen of California. Delahunty is a Google
18 Customer who uses the Internet, including websites from which Google sold and shared Google
19 Customer information without authorization, as alleged herein. Delahunty uses the Chrome web
20 browser, including to search for and watch audio-visual materials. In order to become a Google
21 Customer, Delahunty was required to indicate she agreed to Google’s contractual terms and
22 conditions. On information and belief, unbeknownst to Delahunty at the time, Google sold and
23 shared her personal information in Google RTB auctions on thousands of occasions over the
24 years to thousands of unknown auction participants.

25 29. Plaintiff Meghan Cornelius is a citizen of Texas. Cornelius is a Google Customer
26 who uses the Internet, including websites from which Google sold and shared Google Customer
27

28 _____
¹⁵ *See* Google Terms of Service dated Apr. 14, 2014, Oct. 25, 2017, and Mar. 31, 2020.

1 information without authorization, as alleged herein. Cornelius uses the Chrome web browser,
2 including to search for and watch audio-visual materials. In order to become a Google Customer,
3 Cornelius was required to indicate she agreed to Google's contractual terms and conditions. On
4 information and belief, unbeknownst to Cornelius at the time, Google sold and shared her
5 personal information in Google RTB auctions on thousands of occasions over the years to
6 thousands of unknown auction participants.

7 30. Plaintiff John Kevranian is a citizen of California. Kevranian is a Google
8 Customer who uses the Internet, including websites from which Google sold and shared Google
9 Customer information without authorization, as alleged herein. Kevranian uses the Chrome web
10 browser, including to search for and watch audio-visual materials. In order to become a Google
11 Customer, Kevranian was required to indicate he agreed to Google's contractual terms and
12 conditions. On information and belief, unbeknownst to Kevranian at the time, Google sold and
13 shared his personal information in Google RTB auctions on thousands of occasions over the
14 years to thousands of unknown auction participants.

15 31. Because of the ubiquity of Google's advertising services to businesses and its
16 surveillance technologies, it is practically impossible for any American to use the Internet
17 without their personal information being subject to Google RTB.

18 32. On information and belief, Google has sold and shared the personal information
19 of Plaintiffs and tens of millions of other Americans in Google RTB auctions on countless
20 occasions over the years to unknown auction participants, including information about the audio-
21 visual materials they requested, obtained and watched on the Chrome browser which was sold
22 and shared in Google's RTB auctions without express written consent.

23 33. Google is a limited liability company headquartered in Mountain View,
24 California. Google is owned by Alphabet Inc., a publicly traded company headquartered in
25 Mountain View, California. Alphabet trades under the stock trading symbols GOOG and
26 GOOGL. Alphabet's revenues are primarily due to Google's delivery of targeted advertising that
27 is driven by Google's RTB auction process. Google engages in, and its activities substantially
28 affect, interstate trade and commerce. Google provides a range of products and services that are

1 marketed, distributed, and offered to consumers throughout the United States.

2 **IV. FACTS**

3 **G. Google Falsely Represents That It Protects Its Customers' Privacy**

4 34. According to Pew Research Center nearly all Americans believe it is important to
5 be “in control of who can get information” about them; to not be tracked without their consent;
6 and to be in “control[] of what information is collected about [them].”¹⁶

7 35. Google’s own researchers have confirmed that consumers are more likely to trust
8 a company when the consumers believe they have control over how the company uses their
9 information. In 2016, Google researcher Martin Ortlieb published a research paper titled
10 “Sensitivity of personal data items in different online contexts,”¹⁷ and other Google researchers
11 have since explained the need for transparency regarding how user information is handled.¹⁸
12 Google researchers have explained that when users are more likely to freely share their
13 information when trust is established and they believe they are in control of whether and how
14 their personal information is being used; it’s a matter of trust.¹⁹

15 36. To instill trust, Google repeatedly has held itself out as a champion of Internet
16 privacy. For example, on June 6, 2016, a coalition of technology companies and privacy
17 advocates united to oppose Congressional efforts to expand government surveillance of online by
18 signing a joint letter with the ACLU, Amnesty International and other NGOs, taking the position
19 that online surveillance without court oversight raises “civil liberties and human rights concerns”
20 because it the information obtained “would paint an incredibly intimate picture of an individual’s

21
22 ¹⁶ <https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/>

23 ¹⁷ Martin Ortlieb and Ryan Garner, *Sensitivity of personal data items in different online*
24 *contexts*, De Gruyter Oldenbourg (June 3, 2016) available at
25 <https://www.degruyter.com/document/doi/10.1515/itit-2016-0016/html> (Last Visited Apr. 26, 2021).

26 ¹⁸ Igor Bilogrevic and Martin Ortlieb, “*If You Put All The Pieces Together...*” – *Attitudes*
27 *Towards Data Combination and Sharing Across Services and Companies*, CHI Conference
28 on Human Factors in Computing Systems (May 2016), available at
<https://dl.acm.org/doi/pdf/10.1145/2858036.2858432> (Last Visited Apr. 26, 2021).

¹⁹ Martin Ortlieb, et al., *Trust, Transparency & Control in Inferred User Interest Models*, CHI Extended Abstracts on Human Factors in Computing Systems (April 2014).

1 life” that would include “browsing history, email metadata, location information, and the exact
2 date and time a person signs in or out of a particular online account” which would “reveal details
3 about a person’s political affiliation, medical conditions, religion, substance abuse history, sexual
4 orientation” and even physical movements.²⁰

5 37. Google also stated that beginning in August 2020, it would restrict advertising for
6 “products or services that are marketed or targeted with the express purpose of tracking or
7 monitoring another person or their activities without their authorization,” because such
8 nonconsensual surveillance of “browsing history” is “dishonest behavior.”²¹

9 38. Google’s recognition of the value of trust on the issue of Internet privacy
10 underscores its awareness of the materiality of its repeated false statements and omissions which
11 give Google customers a false impression of safety and control over their data.

12 39. Google represents: “When you use our services, you’re trusting us with your
13 information. We understand this is a big responsibility and work hard to protect your
14 information[.]”²²

15 40. On December 11, 2018, Google CEO Sundar Pichai testified before Congress
16 and repeated Google’s promise, “**We do not and would never sell consumer data.**”²³

17 41. On May 7, 2019, Pichai published an opinion piece in the New York Times,
18 stating: “**To make privacy real, we give you clear, meaningful choices around your data.**
19 **All while staying true to two unequivocal policies: that Google will never sell any**
20 **personal information to third parties; and that you get to decide how your information is**
21

22
23 ²⁰ June 6, 2016 Joint Letter. Available at
24 <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>

25 ²¹ https://support.google.com/adspolicy/answer/9726908?hl=en&ref_topic=29265 (last visited
26 Apr. 22, 2021)

27 ²² *E.g.*, Google Privacy Policy dated May 25, 2018; Google Privacy Policy dated Dec. 19, 2019;
28 Google Privacy Policy dated Feb. 4, 2021.

²³ *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).

1 **used”.**²⁴

2 42. On October 28, 2020, during his testimony before the Senate Committee on
3 Commerce, Science and Transportation, Pichai stated: **“Privacy is one of the most important
4 areas we invest in as a company. Have thousands of engineers working on it. We believe
5 in giving users control, choice, and transparency. And anytime we associate data with
6 users, we are transparent.”**

7 43. Google makes these promises and public statements regarding the use of Google
8 Customers’ personal information to create trust, increase user engagement and increase revenue
9 for Google. Higher user engagement means more revenue in that moment for Google (and also
10 more data about the users that can lead to more revenue). By promising more privacy, and failing
11 to deliver on those promises, Google fraudulently induces more data sharing.

12 **H. Google’s History of Privacy Violations & Its Agreement with the Federal
13 Trade Commission**

14 44. Despite its professed commitment to Internet privacy, Google has violated Google
15 Customer’s privacy rights and trust for years.

16 45. In 2010, the FTC charged that Google “used deceptive tactics and violated its own
17 privacy promises to consumers when it launched its social network, Google Buzz.” To settle the
18 matter, the FTC barred Google “from future privacy misrepresentations” and required Google
19 “to implement a comprehensive privacy program.”²⁵

20 46. In 2011, Google entered into a consent decree with the FTC (the “Consent
21 Decree”), effective for 20 years, in which the FTC required and Google agreed as follows
22 (emphasis added):

23 **IT IS ORDERED that [Google], in or affecting commerce,
24 shall not misrepresent in any manner, expressly or by
25 implication: A. the extent to which [Google] maintains and**

26 ²⁴ Pichai, Sundar (May 7, 2019), *Google’s Sundar Pichai: Privacy Should Not Be a Luxury
27 Good*, The New York Times, available at <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html>

28 ²⁵ <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz> (last visited Apr. 22, 2021).

1 protects the privacy and confidentiality of any covered
2 information, including, but not limited to, misrepresentations
3 related to: (1) the purposes for which it collects and uses
4 covered information, and (2) the extent to which consumers
may exercise control over the collection, use, or disclosure of
covered information.²⁶

5 47. This requirement applies to the Google conduct at issue in this lawsuit, as the
6 Consent Decree broadly defines “covered information” to include information Google “collects
7 from or about an individual” including a “persistent identifier, such as IP address,” and
8 combinations of additional data with the same.

9 48. Just one year after the Consent Decree was entered, the FTC found that Google
10 had already violated the Consent Decree, by way of Google’s misrepresentations regarding what
11 consumer data it would and would not collect with the Safari web browser. In an August 2012
12 press release, the FTC explained:

13 **Google Inc. has agreed to pay a record \$22.5 million civil**
14 **penalty to settle Federal Trade Commission charges that it**
15 **misrepresented to users of Apple Inc.’s Safari Internet browser**
16 **that it would not place tracking “cookies” or serve targeted ads**
to those users, violating an earlier privacy settlement between
the company and the FTC.

17 **The settlement is part of the FTC’s ongoing efforts make sure**
18 **companies live up to the privacy promises they make to**
19 **consumers, and is the largest penalty the agency has ever**
20 **obtained for a violation of a Commission order. In addition to**
21 **the civil penalty, the order also requires Google to disable all**
the tracking cookies it had said it would not place on
consumers’ computers.²⁷

22 49. Since 2012, a number of federal, state, and international regulators have similarly
23 accused Google of violating its promises to consumers on what data it would and would not
24 collect, with Google failing to obtain consent for its conduct.

25
26 ²⁶

27 [https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.p](https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf)
df (last visited Apr. 22, 2021).

28 ²⁷ [https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-](https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented)
ftc-charges-it-misrepresented (last visited Apr. 22, 2021).

1 50. In September 2016, when Google updated its browser app for Apple iOS, Google
2 wrote that users would have “[m]ore control with incognito mode” and “Your searches are your
3 business. That’s why we’ve added the ability to search privately with incognito mode in the
4 Google app for iOS. When you have incognito mode turned on in your settings, your search and
5 browsing history will not be saved.”²⁸ Similarly, in May 2018, Google modified its privacy
6 policy to state, “[y]ou can use our services in a variety of ways to manage your privacy. . . . You
7 can also choose to browse the web privately using Chrome in Incognito mode.”²⁹

8 51. Google made no statements about how users’ privacy would actually be limited in
9 these private browsing sessions and avoided disclosing that users’ information was being
10 collected while they are in private browsing mode through means that include Google Analytics,
11 Google fingerprinting techniques, concurrent Google applications and processes on a consumer’s
12 device and Google’s Ad Manager.

13 52. In 2019, Google and YouTube agreed to pay \$170 million to settle allegations by
14 the Federal Trade Commission and the New York Attorney General that YouTube video sharing
15 services illegally collected personal information from children without their parents’ consent.

16 53. Then, in June 2020, France’s Highest Administrative Court upheld a 50 million
17 Euro fine against Google based on its failure to provide clear notice and obtain users’ valid
18 consent to process their personal data for ad personalization purposes.

19 54. There is currently an ongoing proceeding by the Arizona Attorney General
20 alleging Google failed to obtain consent regarding its collection of location data and its decision
21 to combine certain user data. In the Arizona Attorney General action, Google has produced
22 documents establishing “overwhelming” evidence that “Google has known that the user
23 experience they designed misleads and deceives users.”

24
25
26
27 ²⁸ <https://www.googblogs.com/the-latest-updates-and-improvements-for-the-google-app-for-ios/>
(last visited Apr. 22, 2021).

28 ²⁹ <https://policies.google.com/privacy/archive/20171218-20180525?hl=en-US> (last visited Apr.
22, 2021).

1 55. Google’s employees made numerous admissions in internal communications,
2 recognizing that Google’s privacy disclosures are a “mess” with regards to obtaining “consent”
3 for its data collection practices and other issues relevant in this lawsuit.

- 4
- 5 • **“Do users with significant privacy concerns understand what data we are saving?”**
 - 6 • **“[T]ake a look at [redacted by Google] – work in progress, trying to rein in the overall mess that we have with regards to data collection, consent, and storage.”**
 - 7
 - 8 • **“[A] bunch of other stuff that’s super messy. And it’s a Critical User Journey to make sense out of this mess.”**
 - 9

10 56. Those internal documents, which are heavily redacted, demonstrate that Google
11 employees have voiced their view that Google in fact does not inform Google Customers and
12 Google Customers have not provided informed consent about how their information is collected
13 and used by Google.

14 57. And most recently, Australia’s federal court is reported to have concluded that
15 Google misled consumers about personal data collected through Android mobile devices. The
16 Australian Competition and Consumer Commission, a regulator, reportedly will seek a penalty in
17 the “many millions.”³⁰

18 **I. Google Promises That It Doesn’t Sell Customers’ Personal Information**

19 58. To access many of Google’s products a Google Customer must open a Google
20 Account.³¹ To open a Google Account the Google Customer must indicate they agree to
21 Google’s Terms of Service (“TOS”).³²

22 59. The TOS designates California law as governing law and Google is bound by
23 California’s definition of the term “personal information.” Under California law personal

24 ³⁰ <https://www.reuters.com/technology/australia-finds-google-misled-customers-over-data-collection-regulator-2021-04-16/> (last visited Apr. 22, 2021).

25 ³¹ Google Account Help, Create A Google Account,
26 <https://support.google.com/accounts/answer/27441?hl=en&ref topic=3382296>. (last visited Apr. 21, 2021).

27 ³² Though the Terms of Service at issue are materially identical throughout the Class Period, the manner
28 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 information is “information that identifies, relates to, describes, is reasonably capable of being
2 associated with, or could reasonably be linked, directly or indirectly, with a particular consumer
3 or household.” Cal. Civ. Code § 1798.140(v)(1).

4 **1. The Privacy Policy Provided Personal Information Was Not Shared or Sold**

5 60. Google Customers who created a Google Account prior to around May 2018 were
6 required to agree to both the TOS and the Google Privacy Policy (the “Privacy Policy”).

7 61. The Privacy Policy made promises to Google Customers throughout the Class
8 Period regarding the protection of their personal information.

9 62. The Privacy Policy tracks the California Statutory definition of “personal
10 information,” defining it as “information that you provide to us which personally identifies you,
11 such as your name, email address, or billing information, or other data that can be reasonably
12 linked to such information by Google, such as information we associate with Google Account.”³³

13 63. The Privacy Policy describes the information it associates with Google Accounts,
14 i.e. “personal information,” to include the following:

15 The information we collect includes unique identifiers, browser
16 type and settings, device type and settings, operating system,
17 mobile network information including carrier name and phone
18 number and application version number. We also collect
19 information about the interaction of your apps, browsers, and
20 devices with our services, including IP address, crash reports,
21 system activity and the date, time, and referrer URL at your
22 request.³⁴

23 64. The document at the “unique identifiers” hyperlink defines a unique identifier as
24 “a string of characters that can be used to uniquely identify a browser, app, or device,” which
25 includes cookies, advertising ids and other unique device identifiers.³⁵

26 65. Google associates these unique identifiers—cookies, IP addresses, User-Agent
27 information, advertising IDs, other unique device identifiers, and browsing history information—
28 with individual accounts that include names, email addresses, geolocation, and all other

³³ See Google Privacy Policy dated Dec. 19, 2019.

³⁴ See, e.g., *id.*

³⁵ See, e.g., *id.*

1 information Google maintains on individual account holders.

2 66. But Google expressly assures Google Customers that personal information will
3 not be shared with third parties without Google Customers' consent. Specifically, the Privacy
4 Policy makes promises that Google doesn't share information that personally identifies you with
5 advertisers;³⁶ and that it doesn't share the Google Customers' personal information with
6 companies except with their consent.³⁷ Google has also promised that it doesn't show Google
7 Customers personalized ads based on sensitive categories, such as race, religion, sexual
8 orientation, or health."³⁸

9 67. Where the Privacy Policy mentions sharing information with "partners," it
10 emphasizes and promises that the information shared is not personally identifiable.³⁹

11 68. But that provision is misleading. First, it describes "non-personally identifiable
12 information" as "information that is recorded about users so that it no longer reflects or
13 references an individually-identifiable user;"⁴⁰ a definition that conflicts with California law and
14 with Google's own statement that the data associated with individual Google Customers is
15 "personal information," regardless of whether it "no longer reflects or references an individual
16 user."⁴¹

17 69. Second, Google expressly limits collection of "information from your browser or
18 device for advertising and measurement purposes" to "specific partners" listed in a hyperlink and
19 promises that such information is limited to "non-personally identifiable information."⁴² The
20 hyperlink repeats the false promise that: "We don't share information that personally identifies
21

22 _____
23 ³⁶ *E.g.*, Google Privacy Policy dated May 25, 2018 at 5; Google Privacy Policy dated Dec. 19,
2019.

24 ³⁷ *E.g.*, Google Privacy Policy dated June 28, 2016 at 6; Google Privacy Policy dated Dec. 19,
2019.

25 ³⁸ *E.g.*, Google Privacy Policy dated May 25, 2018 at 5; Google Privacy Policy dated Dec. 19,
2019.

26 ³⁹ *E.g.*, *Id.*

27 ⁴⁰ *E.g.*, *Id.*

28 ⁴¹ *E.g.*, *Id.*

⁴² *Who are Google's Partners?*, Google, <https://policies.google.com/privacy/google-partners>
(last visited Apr. 21, 2021).

1 you with our advertising partners[.]”⁴³

2 2. Terms of Service from May 2018 to the Present

3 70. Google Customers who created a Google Account from around May 2018 to
4 present, were required to agree only to the TOS. While Google Customers were not required to
5 agree to the Privacy Policy during this period, creating a Google Account included a link to the
6 Privacy Policy to show how Google would “process your information.”⁴⁴ The Privacy Policy
7 during this time contained repeated promises regarding how Google would use Google
8 Customers’ information.

9 71. While the TOS refers to the Privacy Policy, from March 31, 2020 to present, the
10 TOS also states that the Privacy Policy is “not part of these terms.”⁴⁵ During this period, the
11 TOS incorporated a hyperlink to the “How our business works” webpage.

12 72. The TOS, since March 31, 2020, have stated, “You have no obligation to provide
13 any content to our services and you’re free to choose the content that you want to provide.”⁴⁶

14 73. In the TOS, the reference and hyperlink: to “the way Google's business works”
15 takes the Google Customer to Google’s “How our business works” page, thereby incorporating
16 that linked document into the TOS. On the very first page of that linked document, Google
17 declares in large type: **“We don’t sell your personal information to anyone.”**
18 Google also states, “[W]e never sell your personal information to anyone[.]”⁴⁷

19 74. The “How our business works” page further promises: “Advertisers do not pay
20 us for personal information[.]”; “[W]e never share that information with advertisers, unless you
21 ask us to.”; “We also never use your emails, documents, photos, or sensitive information like
22 race, religion, or sexual orientation, to personalize ads to you.” “We share reports with our
23 advertisers to help them understand the performance of their ads, but we do so without revealing
24 any of your personal information.” “At every point in the process of showing you ads, we keep

25
26 ⁴³ *Id.*

27 ⁴⁴ *See, e.g., Tom Leeman, How to create a Google Account, YouTube* (Feb. 2, 2020)
https://youtu.be/ArZpwBl_z10 (at 4:40-4:45).

28 ⁴⁵ *See* Google Terms of Service dated Mar. 31, 2020.

⁴⁶ *See* Google Terms of Service dated Mar. 31, 2020.

⁴⁷ <https://about.google/how-our-business-works/> (last visited Apr. 29, 2021)

1 your personal information protected with industry-leading security technologies.”⁴⁸

2 75. In addition to the promises made in contractual documents of Google’s TOS
3 and Privacy Policy, Google has made other similar misrepresentations on its website in the
4 “Who are Google’s Partners” webpage; the Google Personalized Advertising webpage, the
5 “We do not Sell your personal information to anyone” webpage, and the “Your privacy is
6 protected by responsible data practices” webpage. These representations all pertain to
7 Google’s repeated false promise that it doesn’t share information that personally identifies
8 the Google Customer with their advertising partners.

9 76. Finally, Google collects Google Customers’ personal information under false
10 pretenses. Google promises Google Chrome users that they “don’t need to provide any
11 personal information to use Chrome” and that “[t]he personal information that Chrome
12 stores won’t be sent to Google unless you choose to store that data in your Google Account
13 by turning on sync[.]”⁴⁹ Despite these promises, regardless of whether or not a Google
14 Customer elects to synchronize their Google account and Google Chrome, Google Chrome
15 sends Google Customers’ personal information to Google, which information is then sold in
16 Google’s RTB auction process.

17 **J. Google Real-Time Bidding is Hidden to Google Customers**

18 77. The Google Ad Exchange is a digital auction house that provides a platform for
19 placing targeted ads on users’ web browsers and devices. Through the Google’s RTB auctions on
20 its Ad Exchange, Google shares and sells Google Customers’ personal information with Google
21 RTB auction participants to solicit bids for the right to display a real-time. The Google RTB
22 auction ad exchange is the largest in the world, estimated to be responsible to 53 percent of all
23 RTB transactions globally.

24 78. Google’s RTB auction process is misleadingly disclosed and otherwise hidden to
25 Google Customers. It is called real time bidding because it occurs almost instantaneously. It is
26

27 ⁴⁸ *Id.*

28 ⁴⁹ Google Chrome Privacy Notice; *available at*: <https://www.google.com/chrome/privacy/> (last visited May 4, 2021).

1 an automated system that is invisible to Google Customers, which repeated sells their personal
2 information to hundreds of participants.

3 79. The information about Google Customers passes through a complex series of
4 layers of demand-side platform and supply-side platforms in what is referred to as an “Ad Stack”
5 as the data published by Google to numerous third parties. The Ad Stack proceeds as follows.
6 First, the publisher is the website that has ad space to sell. Second, the supply side platform
7 (“SSP”) is a separate entity that collects the Google Customer information to sell and the
8 information about the ad space to be filled. Third, the ad exchange organizes the auctions
9 between buyer and seller. Fourth, the demand-side platform (“DSP”) submits bids on behalf of
10 advertisers for the ad space. Finally, fifth the advertiser purchases ads targeted to specific Google
11 Customers. Google controls the Ad Stack in Google RTB auctions because Google controls
12 significant players at the SSP, ad exchange, and DSP layers of the Ad Stack.

13 80. An example illustrates the process. Medical Website reserves advertising space
14 on its web pages to sell through Google RTB. A Google Customer looks for a specific page, in
15 this example an article on Medical Website on breast cancer, by entering the web address in the
16 navigation bar of his or her web browser and hits “enter.” This triggers the web browser to send
17 a request to Medical Website, which, in turn, responds by displaying the Medical Website article
18 on the Google Customer’s browser or device. As internet users are accustomed to, the requested
19 webpage will display in a matter of seconds. But the Google Customer is unaware that the
20 request to view the Medical Website article on breast cancer is also accompanied by a “cookie,”
21 which is sent from the Google Customer’s web browser to the SSP which collects that and other
22 Google Customer information to sell ad space for advertising associated with and on that
23 Medical Website page.

24 81. If the SSP is AdMob (i.e., “Advertising on Mobile”), an entity which is owned by
25 Google, Google/AdMob matches the cookie to the Google Customer’s personal information
26 stored by Google. Due to its immense storage of individual personal information,
27 Google/AdMob has a practically unlimited ability to connect cookies to personal information.
28 From its vast data set on each Google Customer, Google creates a Bid Request – containing the

1 Google Customer’s personal information and the content of the specific article that is the subject
 2 of the Google Customer’s interest. This Bid Request is then sent to DSP participants of the
 3 Google RTB auction (DSPs bid on behalf of advertisers). All Google RTB auction participants
 4 can review, save and use the personal information in the Bid Request. Bids are submitted and the
 5 highest bidder wins the bid and places its ad on Medical Website’s webpage containing the
 6 breast cancer article which the Google Customer is viewing. This process will repeat every time
 7 the user clicks another hyperlink to continue her research on breast cancer; resulting in ever more
 8 personal information exchanged on Google’s RTB auction.

10 **1. How Google Customers’ Personal Information is Shared on the RTB Auction**

11 82. The personal information about a Google Customer is the key item for sale based
 12 on the order in which the re-directed data is provided from Google to the bidders:⁵⁰ Under the
 13 RTB, data is shared under the following categories, according to Google:

- 14 • “[I]nformation that we know about the user,” which includes, among other things, IP
 15 address, Google ID, and user verticals;
- 16 • “[I]nformation that we know about the webpage or mobile app,” which includes, among
 17 other things, publisher ID, detected verticals, vertical weight, and content labels;
- 18 • Auction information, including a unique ID for the overall query, and the type of auction
 19 that will be run for this query;
- 20 • “Information about the device,” which includes, among other things, the type (e.g.,
 21 phone, desktop, tablet), platform (e.g., Android, iPhone), brand, model, and operating
 22 system;
- 23 • “Information for ad queries coming from mobile devices,” which includes, among other
 24 things, whether the request is coming from a smartphone or tablet, and information about
 25 the mobile app.

26 83. “Vertical” information is also transmitted by Google to define that Google

27
 28 ⁵⁰ <https://developers.google.com/authorized-buyers/rtb/downloads/realtime-bidding-protocol>
 (last visited Apr. 23, 2021).

1 Customer's advertising segment, including, but not limited to, sexuality, ethnicity, religion, and
2 health conditions. This "vertical" information, which is made up of the personal information
3 Google has persistently collected on each individual Google Customer, constitutes personal
4 information under both California law and Google's express policies. The information shared by
5 Google through its RTB auction is personal information that is reasonably capable of being
6 associated, or that could reasonably be linked, directly or indirectly, with a particular consumer
7 or household. Cal. Civ. Code § 1798.140(o)(1). In fact, bidders routinely associate this personal
8 information with the consumer it describes so intimately. Google's unlawful dissemination and
9 sale of this highly personal vertical information violates its privacy promises, and constitutes an
10 invasion of Google Customers' reasonable expectation of privacy and right to privacy.

11 **2. Google's Disclosures Are Personally Identifiable to RTB Participants**

12 84. Google represents that any information it has collected about a Google Customer
13 is "anonymized" and that it is shared to "just a few partners." In fact, unique identifiers allow
14 RTB auction participants to match the personal information that Google transactionally shares
15 with their own information. This results in increasingly large dossiers on each individual Google
16 Customer. RTB participants are also able to infer sensitive verticals about an individual based
17 on their web activity, where they are located and what they purchase, which is provided by
18 Google.

19 85. Google allows the disclosure of personally identifiable information to RTB
20 auction participants in two ways. First, Google provides publishers with personal information
21 that they use to specifically identify the Google Customer for the purpose of bidding on an ad in
22 Google's Ad Exchange. This is to say, Google provides personal information to an advertiser
23 who bid on an ad in the ad exchange.

24 86. Second, whether or not advertiser submits a winning bid, participating in the
25 auction facilitates the acquisition and retention of Google Customers' personal information that
26 Google RTB participants use to create or continuously update and augment their own existing
27 user data troves.

28 87. Third, Google assists Google RTB auction participants to connect Google

1 Customer personal information made available in a Bid Request to the information those
 2 participants already have about specific individuals through a “cookie matching service.”
 3 “Cookie matching enables Google RTB participants to match their own cookie—for example, an
 4 ID for a user that browsed your website—with a corresponding bidder-specific Google User ID,
 5 and construct user lists that can help the bidder make more effective bidding choices.”⁵¹

6 88. Even though Google Customers are told that the Google ID is anonymous,
 7 through cookie matching, whenever the Google Customer also has an account id with the auction
 8 participant, cookie matching enables that participant to tie the personal information from Google
 9 RTB together with data it already has to enhance its profile of the Google Customer.

10 89. Google promotes the construction of “user lists” that enable Google RTB auction
 11 participants to identify specific Google Customers even when the Google Customer has taken
 12 steps to avoid Google’s tracking of the activity. Google “recommend[s] that bidders instead store
 13 and look up list ids using either google user id or hosted match data as keys.”⁵²

14 90. Google facilitates the identification of individual Google Customers through its
 15 cookie matching service which “allows one to populate user lists”⁵³ and enables the bidder to
 16 match their cookies with Google’s, such that they can determine whether an impression sent in a
 17 bid request is associated with one of users being targeted.”⁵⁴

18 91. Through Google’s use of cookie matching, Google RTB auction participants are
 19 provided with personal information which can be and is used build detailed individual user
 20 profiles regarding Google Customers based on their browsing history.

21 3. Companies Buy and Google Sells Google Customers’ Personal Information

22 92. The Ad Exchange is an opaque system that is not known to Google Customers. It
 23 exists in a virtual space, and not in a physical auction room. Google does not tell Google
 24 Customers which companies are bidding on their personal information, and therefore accessing,

25 _____
 26 ⁵¹ Cookie Matching, <https://developers.google.com/authorized-buyers/rtb/cookie-guide>. (last visited
 Apr. 21, 2021).

27 ⁵² Real-Time Bidding Protocol Buffer v.203, [https://developers.google.com/authorized-
 buyers/rtb/downloads/realtime-bidding-PROTO](https://developers.google.com/authorized-buyers/rtb/downloads/realtime-bidding-PROTO) (last visited Apr. 22, 2021).

28 ⁵³ *Id.*

⁵⁴ *Id.*

1 their personal information, and which companies are winning the RTB auctions. Google
2 disclose portions of this information to hundreds of Google RTB auction participants.

3 93. Google is not required under U.S. law to publish such information to American
4 consumers. This information was reportedly obtained by the creation and deployment of web-
5 crawling scripts.

6 94. However, other data protection jurisdictions do require some transparency into
7 who is buying Google Customers' personal information. Disclosures and reports from those
8 other jurisdictions indicate that the current reports and allegations regarding Google in the U.S.
9 may dramatically underestimate participation in Google RTB and the number of entities to which
10 Google sells Google Customers' personal information.

11 95. The European Union, for example, has different laws and requires Google to
12 identify all companies with which it shares personal data in the European Economic Area. The
13 published list includes 833 companies, including well-known companies like Amazon,
14 Facebook, Twitter, Microsoft (LinkedIn), Netflix, Adobe, Oracle, Salesforce, and eBay, as well
15 as hundreds of little-known companies.⁵⁵ Similarly, a study submitted to the Irish Data
16 Protection Commission estimated that an estimated 13.5 million websites participated in the
17 Google RTB and 2,182 companies directly received Google RTB data.⁵⁶

18 96. As stated in one complaint to the EU's Data Protection Commission, real-time
19 bidding represents a "vast systematic data breach" that allows data brokers to "develop intimate
20 profiles about us, our afflictions and interests" for sale.⁵⁷

21 97. On January 22, 2021, the United Kingdom's Information Commissioner's Office
22 announced that it was resuming its investigation into RTB, stating: "The complex system of RTB
23 can use people's sensitive personal data to serve adverts and requires people's explicit consent,
24 which is not happening right now. . . . Sharing people's data with potentially hundreds of
25

26 ⁵⁵ <https://support.google.com/admanager/answer/9012903?hl=en> (last visited Apr. 22, 2021)

27 ⁵⁶ 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.

28 ⁵⁷ See <https://www.irishtimes.com/business/technology/data-privacy-advocate-submits-further-evidence-in-google-ads-inquiry-1.4359853> (last visited May 2, 2021).

1 companies, without properly assessing and addressing the risk of these counterparties, also raises
2 questions around the security and retention of this data.”⁵⁸

3 98. Complaints filed with the Irish Data Protection Commission detail the categories of
4 sensitive personal information published in Google’s RTB process, including political information,
5 and health categories, such as “Substance abuse,” “Diabetes,” “Chronic Pain” “Sleep Disorders,”
6 “AIDS & HIV,” “Incest & Abuse Support,” “Brain Tumor,” “Incontinence” and “Depression.”⁵⁹

7 **4. Statute of Limitations is Tolled**

8 99. Google’s RTB process is hidden to the Plaintiffs and Google Customers. The
9 Terms of Service does not inform Plaintiffs and Google Customers that Google’s advertising
10 services discloses their personal information as alleged herein. Google continues to conceal this
11 information.

12 100. An average consumer could not reasonably be expected to know or understand
13 how Google is using their data. The developer pages cited herein, while available on the web, are
14 not easily understandable to the average person, and even those pages do not fully reveal the
15 extent of Google’s actions.

16 101. Plaintiffs were not aware of the factual bases for their claims for relief despite
17 reasonable diligence. Thus, the statutes of limitation have been tolled by Google’s fraudulent
18 concealment and denial of the facts alleged herein through the time period relevant to this action.

19 **K. Google has been wrongly enriched by its conduct**

20 102. Google’s monetizes the value of Internet users’ personal information. This is
21 reflected by Google’s advertisement revenue. Google reported \$146.9 billion in advertising
22 revenue in 2020, \$134.8 billion in 2019, \$116.3 billion in 2018, \$95.4 billion in 2017, and \$79.4
23 billion in 2016.⁶⁰ This translates to 83% of Google’s total revenues in 2019, 85% in 2018, 86%

25 ⁵⁸See ICO Statement, *Adtech investigation resumes*; available at: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/01/adtech-investigation-resumes/> (last visited 5.5.21)

26 ⁵⁹See TechCrunch, *Ireland’s data watchdog slammed for letting adtech carry on ‘biggest breach of all time’* available at: <https://techcrunch.com/2020/09/21/irelands-data-watchdog-slammed-for-letting-adtech-carry-on-biggest-breach-of-all-time/> (last visited 5.5.21)

27 ⁶⁰2018 Annual Report, Alphabet Inc. (Feb. 4, 2019), <https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm> (hereinafter “2018 Annual Report”).

1 in 2017 and 88% in 2016.⁶¹ Some large portion of information collected and sold by Google is
2 included in these revenue figures.

3 103. Google's data mining of Google Customers' personal information has also helped
4 the revenues of Google's associates, which include ads placed through Google's partnered ad
5 exchanges. Google reported the following revenues from Google associate properties: \$21.5
6 billion in 2019, \$20 billion in 2018, \$17.6 billion in 2017, and \$15.6 billion in 2016.⁶² Google
7 reports "strength in both AdMob and AdManager" primarily led to the \$2.4 billion increase in
8 Google associate properties revenues from 2017 to 2018.⁶³

9 104. Advertising auctions confirm that the personal information Google sells to RTB
10 participants has economic value. The value of Americans' personal information gathered and
11 used by Google has been reported to be valued at \$21.5 billion in 2018.⁶⁴

12 105. Further, participants in the auction who don't place advertisements are
13 incentivized to participate in the RTB auction solely to data mine consumer information in order
14 to monetize that information.

15 **L. Plaintiffs' personal information is property under California law**

16 106. Data or communications is considered property under California law because it is
17 an intangible thing a person has a right to possess, use or enjoy. Google Customers have a
18 property interest in their own data and personal information.

19 107. The California Consumer Privacy Act permits businesses to purchase consumer
20 information from consumers themselves, *see* Cal. Civ. Code § 1798.125(b)(1), and permits
21 businesses to assess and appraise—i.e., to place a monetary value on—consumer data. *See* Cal.

22
23 ⁶¹ 2019 Annual Report, Alphabet Inc. (Feb. 3, 2020), [https://www.sec.gov/Archives/edgar/
24 data/1652044/000165204420000008/goog10-k2019.htm](https://www.sec.gov/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm) (hereinafter "2019 Annual
Report"); 2018 Annual Report.

25 ⁶² 2019 Annual Report; 2018 Annual Report.

26 ⁶³ 2019 Annual Report.

27 ⁶⁴ Robert Shapiro and Siddhartha Aneja, *Who Owns Americans' Personal Information and What
Is It Worth?*, Future Majority (April 2019), available at [https://futuremajority.org/wp-
28 content/uploads/PersonalInfo.pdf](https://futuremajority.org/wp-content/uploads/PersonalInfo.pdf). Shapiro is a Senior Policy Fellow at the Georgetown
University McDonough School of Business and, among other past positions, served as the
U.S. Under-Secretary of Commerce for Economic Affairs under President Clinton.

1 Civ. Code §1798.125(a)(2)).

2 108. But for Google hiding how it was actually using Google Customers' personal
3 information the number of Google customers would have declined which would have hurt
4 Google's bottom line. Google avoided these costs by secretly robbing Google Customers of the
5 value of their personal information.

6 109. Google unlawfully and secretly diverted Google Customers' personal information
7 to realize billions in profits by misrepresenting what they were going to do with it, and how it
8 was going to be disclosed. Accordingly, Plaintiffs and Google Customers were injured.

9 **M. The California Financial Privacy Act Imposes Information Fiduciary**
10 **Obligations Upon Google**

11 110. For years, scholars have recognized that the law should recognize "information
12 fiduciaries,"⁶⁵ and have singled out the California Consumer Privacy Act ("CCPA") as
13 legislation modeling how to impose such duties.⁶⁶

14 111. "An information fiduciary is a person or business who, because of their
15 relationship with another, has taken on special duties with respect to the information they obtain
16 in the course of the relationship."⁶⁷ Google is listed as a prime example of an information
17 fiduciary.⁶⁸

18 112. "People and business entities act as information fiduciaries (1) when these people
19

20
21 ⁶⁵ "[M]any online service providers and cloud companies who collect, analyze, use, sell, and
22 distribute personal information should be seen as information fiduciaries toward their
23 customers." Jack M. Balkin, Information Fiduciaries and the First Amendment (2016) 49 U.C.
24 Davis L. Rev. 1183, 1186. See also Alicia Solow-Niederman, Beyond the Privacy Torts:
25 Reinvigorating a Common Law Approach for Data Breaches, 127 YALE L.J.F. 614, 628 (2018),
26 https://www.yalelawjournal.org/pdf/Solow-Niederman_qthw8784.pdf [<https://perma.cc/LSR8-32G2>]; Matthew S. DeLuca, The Hunt for Privacy Harms After Spokeo, 86 FORDHAM L.
27 REV. 2439, 2460 (2018).

28 ⁶⁶ "The proposed California Consumer Privacy Act of 2018 is an interesting model for this kind
of legislation" which would impose information fiduciary obligations on companies collecting
consumer data. Ariel Dobkin, Information Fiduciaries in Practice: Data Privacy and User
Expectations (2018) 33 Berkeley Tech. L.J. 1, 48.

⁶⁷ Jack M. Balkin, Information Fiduciaries and the First Amendment (2016) 49 U.C. Davis L.
Rev. 1183, 1186.

⁶⁸ *Id.*

1 or entities hold themselves out to the public as privacy-respecting organizations in order to gain
2 the trust of those who use them; (2) when these people or entities give individuals reason to
3 believe that they will not disclose or misuse their personal information; and (3) when the affected
4 individuals reasonably believe that these people or entities will not disclose or misuse their
5 personal information based on existing social norms of reasonable behavior, existing patterns of
6 practice, or other objective factors that reasonably justify their trust.”⁶⁹

7 113. In California, “[w]hether a fiduciary duty exists is generally a question of law.
8 Whether the defendant breached that duty towards the plaintiff is a question of fact.” (Marzecv.
9 Public Employees’ Retirement System (2015) 236 Cal.App.4th 889, 915 [187Cal.Rptr.3d 452],
10 internal citation omitted.).

11 114. The CCPA imposes information fiduciary obligations on Google because it
12 imposes special duties on Google with respect to the information it obtains in the course of a
13 relationship with a user—namely, the CCPA requires Google to disclose how it uses consumer
14 Personal Information. Google “shall, at or before the point of collection, inform consumers as to
15 the categories of personal information to be collected and the purposes for which the categories
16 of personal information shall be used. A business shall not collect additional categories of
17 personal information or use personal information collected for additional purposes without
18 providing the consumer with notice consistent with this section.” Cal. Civ. Code, § 1798.100
19 (emphasis added).

20 115. Moreover, Google acts as an information fiduciary because it (1) holds itself out
21 to the public as a privacy-respecting organization in order to gain the trust of those who use it;
22 (2) gives individuals reason to believe that it will not disclose or misuse their personal
23 information; and (3) Google’s consumers, including Plaintiff and Class Members, reasonably
24 believe that Google will not disclose or misuse their personal information-based Google’s
25 representations.

26 116. Google has breached its information fiduciary obligations by misrepresenting how
27
28

⁶⁹ *Id.* at 1223–1224

1 it uses personal information of its consumers, in a manner that allows consumers to be tracked,
2 monitored, surveilled, triangulated, and otherwise watched and manipulated, all without the
3 consumer's consent.

4 **V. CLASS ACTION ALLEGATIONS**

5 117. This is a class action pursuant to Rules 23(a), (b)(2), and (b)(3) (or, alternatively,
6 23(c)(4)) of the Federal Rules of Civil Procedure on behalf of:

7 A Class of all persons residing in the United States with a Google
8 Account who used the Internet using a Chrome browser on or after
9 Google began using RTB in a manner that disclosed Google
Customers' personal information.

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

13 119. The members of the Class are so numerous that joinder of all members is
14 impracticable.

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

- 18 a. Whether Google shared Google Customer personal information with
19 others;
- 20 b. Whether Google sold Google Customer personal information to others;
- 21 c. Whether Google promised not to share personal information with others;
- 22 d. Whether Google promised not to sell personal information to others;
- 23 e. Whether Google was authorized to disclose Google Customer personal
24 information to others;
- 25 f. Whether Google was authorized to sell Google Customer personal
26 information to others;
- 27 g. Whether Google breached its contract with Google Customers;
- 28

- 1 h. Whether Google Customers' Personal Information was improperly sold by
- 2 Google;
- 3 i. Whether Google was unjustly enriched by the unauthorized sales of
- 4 Google Customers' personal information;
- 5 j. Whether Google's actions would be highly offensive to a reasonable
- 6 person;
- 7 k. Whether Google's actions breached the duty of good faith and fair
- 8 dealing;
- 9 l. Whether Google's actions violated the California Unfair Competition
- 10 Law;
- 11 m. Whether Google's actions violated Article I, Section 1 of the California
- 12 Constitution;
- 13 n. Whether Google's actions violated the California Invasion of Privacy Act;
- 14 o. Whether Google's actions violated the Electronic Communications
- 15 Privacy Act;
- 16 p. Whether Google's actions violated the Video Privacy Protection Act;
- 17 q. Whether and the extent to which injunctive relief is appropriate.

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

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

25 123. A class action is superior to all other available methods for the fair and efficient
26 adjudication of this controversy since joinder of all members is impracticable. Furthermore, as
27 the damages individual Class and Subclass members have suffered may be relatively small, the
28 expense and burden of individual litigation make it impossible for members of the Class and

1 Subclass to individually redress the wrongs done to them.

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

3 **VI. CAUSES OF ACTION**

4 **FIRST CLAIM FOR RELIEF**

5 **CALIFORNIA INVASION OF PRIVACY**

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

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

11 127. The phrase “and privacy” was added by an initiative adopted by California voters
12 on November 7, 1972 (the Privacy Initiative). The Privacy Initiative created a private right of
13 action against nongovernmental entities for invasions of privacy.

14 128. The California Supreme Court has explained that, one of the principal “mischiefs”
15 to which the Privacy Initiative was directed was “the overbroad collection and retention of
16 unnecessary personal information by government and business interests.” *White v. Davis*, 13
17 Cal.3d 757, 775 (Cal. 1975).

18 129. Google’s conduct in selling and sharing Plaintiffs’ and Class Members’ personal
19 information violates its promises to the contrary.

20 130. Google creates detailed dossiers of the personal information of Plaintiffs and
21 Class Members, and then sells and shares it with numerous companies to profit and assist those
22 other companies in creating their own separate dossiers about Plaintiffs and Class Members,
23 from which those companies will further profit.

24 131. Plaintiffs and Class Members have the right to privacy in their web-browsing
25 history; in how their personal information is going to be used; in the right to withhold and not
26 disclose their personal information, and all statutory privacy rights codified under federal and
27 California law.

28 132. Google has intruded on these privacy interests.

1 133. Through Google’s contracts and other statement, Google has promised not to
2 share or sell Plaintiffs’ and Class Members’ personal information without their agreement.

3 134. Plaintiffs and Class Members had a reasonable expectation of privacy. Google
4 affirmatively promised users it would not share or sell their personal information without
5 authorization.

6 135. Google’s actions constituted a serious invasion of privacy in that it violates
7 several federal criminal laws, including the Electronic Communications Privacy Act; violates
8 state criminal laws; violates the right to privacy located in the First Amendment of the United
9 States Constitution; invaded the privacy rights of hundreds of millions of Google Customers;
10 disclosed sensitive personal information related to the verticals alleged above; facilitated the
11 disclosure of Google Customers by third parties who did not have legal access to their personal
12 information; and shared and sold personal information of hundreds of millions of Google
13 Customers.

14 136. Google lacked a legitimate business interest in sharing and selling Plaintiffs’ and
15 Class Members’ personal information without their authorization.

16 137. Google acted with oppression, fraud, or malice in invading Plaintiffs’ and Class
17 Members’ privacy.

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

21 **SECOND CLAIM FOR RELIEF**

22 **BREACH OF IMPLIED CONTRACT**

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

24 140. Google created a relationship of trust with Google Customers, such that Google
25 Customers entrusted their personal information to Google.

26 141. Google promised to not sell or share Google Customers, including Plaintiffs’ and
27 Class Members’ personal information.

28

1 142. Google promised to provide Plaintiffs and Class Members with services that did
2 not compromise Google Customers' personal information, rather than providing services that
3 involved Google's knowing sale and sharing of their customers' personal information.

4 143. Google violated its obligation to protect and keep private Plaintiffs' and Class
5 Members' personal information by selling and sharing it to hundreds of companies.

6 144. By doing do, Google breached its implied contracts with Plaintiffs and Class
7 Members.

8 145. Google's failure to fulfill its obligations to honor its obligations to Google
9 Customers resulted in Plaintiffs and Class Members receiving services that were of less value
10 than they provided consideration for.

11 146. Google's failure to keep its promises resulted in Plaintiffs and Class Members
12 suffering economic harm by losing the value of their personal information.

13 **THIRD CLAIM FOR RELIEF**

14 **BREACH OF FIDUCIARY DUTY**

15 147. Plaintiff brings this claim under the California Consumer Privacy Act.

16 148. The California Consumer Privacy Act imposes information fiduciary obligations
17 upon a business that collects a consumer's personal information. That business "shall, at or
18 before the point of collection, inform consumers as to the categories of personal information to
19 be collected and the purposes for which the categories of personal information shall be used. A
20 business shall not collect additional categories of personal information or use personal
21 information collected for additional purposes without providing the consumer with notice
22 consistent with this section." Cal. Civ. Code, § 1798.100 (emphasis added).

23 149. In light of the special relationship between Google and Plaintiffs and Class
24 Members, whereby Google became guardian of Plaintiffs' and Class Members' Personal
25 Information, Google became an information fiduciary by its undertaking and guardianship of the
26 Personal Information, to act primarily for the benefit of its consumers, including Plaintiff and
27 Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Personal Information;
28 (2) to obtain consent for the sale or transmission of such Private Information; and (3) to respect

1 the choices regarding use or sale of the Plaintiffs and Class Members with respect to their
2 Personal Information.

3 150. Google has a fiduciary duty of confidentiality for the benefit of Plaintiffs and
4 Class Members, in particular, to keep the Personal Information of its consumers as secure and
5 confidential as it represents to its consumers.

6 151. Google had information relating to Plaintiffs and Class Members that it knew or
7 should have known was confidential.

8 152. Google used Plaintiffs and Class Members' Personal Information for its own
9 benefit and/or communicated Plaintiffs and Class Members' Personal Information to third parties
10 in a manner that allowed them to be triangulated, identified, tracked, monitored, surveilled and
11 manipulated in a manner Plaintiff and Class Members neither understood nor approved.

12 153. Plaintiffs and Class Members did not give informed consent to Google's conduct.

13 154. The Personal Information was not a matter of general knowledge.

14 155. As a direct and proximate result of Google's breaches of its fiduciary duties,
15 Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:
16 (i) the compromise, publication, and/or theft of their Personal Information; (ii) the continued risk
17 to their Personal Information, which remains in Google's possession and is subject to further
18 unauthorized disclosures so long as Google fails to undertake appropriate and adequate measures
19 to protect the Personal Information in its continued possession; and (iii) future costs in terms of
20 time, effort, and money that will be expended to secure such Personal Information.

21 156. As a direct and proximate result of Google's breaches of its fiduciary duties,
22 Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury
23 and/or harm, and other economic and non-economic losses.

24 **FOURTH CLAIM FOR RELIEF**

25 **UNJUST ENRICHMENT**

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

27 158. Plaintiff brings this claim under the laws of California.

28

1 159. As a result of their unlawful conduct described above, Google has been unjustly
2 enriched.

3 160. Google has been unjustly enriched by the receipt of revenue in connection with
4 the sale and sharing of Plaintiffs’ and Class Members’ personal information.

5 161. Google has benefited from its unlawful acts and it would be inequitable for it to
6 be permitted to retain any of its ill-gotten gains resulting from Plaintiffs’ and Class Members’
7 use of its services.

8 162. Plaintiffs and Class Members are entitled to the amount of Google’s ill-gotten
9 gains resulting from their unlawful, unjust, and inequitable conduct. Plaintiffs and Class
10 Members are entitled to the establishment of a constructive trust consisting of all ill-gotten gains
11 from which Plaintiff and Class Members may make claims on a pro rata basis.

12 **FIFTH CLAIM FOR RELIEF**

13 **VIOLATIONS OF THE CALIFORNIA UNFAIR**

14 **COMPETITION LAW (“UCL”)**

15 **Cal. Bus. & Prof. Code § 17200, et seq.**

16 163. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

17 164. Google is a “person” as defined by Cal. Bus. & Prof. Code § 17201.

18 165. Google violated the UCL by engaging in unlawful, unfair, and deceptive business
19 acts and practices in violation of Cal. Bus. & Prof. Code § 17200.

20 166. Google violated the UCL by violating statutory laws as alleged in this Complaint.
21 This includes, but not limited to, the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510
22 and 2701, et seq.; the Video Privacy Protection Act, 18 U.S.C. § 2710, et seq.; the California
23 Invasion of Privacy Act, Cal. Penal Code §§ 630, et seq.; the California Computer Data Access
24 and Fraud Act, and the Cal. Penal Code § 502.

25 167. Google violated the UCL by violating constitutional and common laws as alleged
26 in this Complaint. This includes, but not limited to the common law right of privacy via
27 intrusion upon seclusion and publication of private facts; the Art. 1, § 1 of the California
28 Constitution Right to Privacy; express contract promises to consumers; the duty of good faith

1 and fair dealing; unjust enrichment; implied contract; and the duty to hold Google Customers'
2 personal information in confidence, and violating its TOS, knowingly and willfully or
3 negligently and materially, in violation of Cal. Bus. & Prof. Code § 22576

4 168. Google violated the UCL by violating the unfair prong, as alleged in this
5 Complaint. This includes, but not limited to violating the spirit and letter of these laws, which
6 protect property, economic and privacy interests, and prohibit unauthorized disclosure and
7 collection of private communications and personal information; and stating it would not sell or
8 disseminate Plaintiffs' and Class Members' personal information without their consent to other
9 companies.

10 169. Plaintiffs' and Class Members' loss of their personal information constitutes an
11 economic injury.

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

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

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

21 **SIXTH CLAIM FOR RELIEF**

22 **INTRUSION UPON SECLUSION**

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

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

26 175. Google intentionally intruded upon the Plaintiffs' and Class Members' solitude or
27 seclusion by (1) monetizing Plaintiffs' and Class Members' personal information without their
28 consent, and (2) by mining and distributing data that they were not authorized to sell or share.

1 176. Google intentionally intruded upon the Plaintiffs' and Class Members' solitude or
2 seclusion by facilitating cookie-matching with hundreds of other companies, as alleged herein. ,
3 Cookie matching enabled companies with limited information about Plaintiffs and other Class
4 Members to accumulate substantially more information about each individual Plaintiff and Class
5 Member from Google.

6 177. Google intentionally intruded upon the Plaintiffs' and Class Members' solitude or
7 seclusion by selling and sharing Plaintiffs' and Class Members' sensitive personal information
8 for purposes of targeted advertising and publicized sensitive information to hundreds of other
9 companies.

10 178. None of Google's actions were authorized by the Plaintiffs and Class Members.

11 179. Google violated federal and state criminal and civil laws designed to protect
12 individual privacy and against theft.

13 180. It is highly offensive to a reasonable person that Google's collected information
14 on the Google Customer's web browsing in order to sell and share it with hundreds of unknown
15 companies without Google Customers' consent. It is also highly offensive that Google shared
16 personal information from Google Customers regarding highly sensitive information, such as an
17 individual's race, ethnicity, religion, health, and financial status.

18 181. It was highly offensive to a reasonable person for Google to intentionally intrude
19 into Plaintiffs' and Class Members personal information, Internet communications, and
20 computing devices.

21 182. Google has acted with oppression, fraud, or malice.

22 183. Plaintiffs and Class Members are entitled to just compensation in the form of
23 actual damages, general damages, unjust enrichment, nominal damages, and punitive damages
24 under this cause of action.

25 **SEVENTH CLAIM FOR RELIEF**

26 **PUBLICATION OF PRIVATE INFORMATION**

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

28 185. Plaintiffs' and Class Members' personal information, including their sensitive

1 data and Internet communications, are private facts that Google promised not to share or sell to
2 advertisers.

3 186. Google publicized Plaintiffs' and Class Members' private facts and the content of
4 their Internet communications by sharing and selling them to hundreds of different companies.

5 187. These companies profit from acquiring personal information and creating vast and
6 rich dossiers to both target advertising and to further sell the personal information to other third
7 parties.

8 188. Plaintiffs and Class Members did not know that Google shared or sold their
9 personal information and did not consent to such publication.

10 189. It is highly offensive to a reasonable person that Google's sold and shared
11 personal information to hundreds of different advertising companies.

12 190. Google acted with oppression, fraud, or malice.

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

16 **EIGHTH CLAIM FOR RELIEF**

17 **BREACH OF CONFIDENCE**

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

19 193. Plaintiffs and Class Members gave their personal information to Google in trust.
20 They trusted Google.

21 194. Plaintiffs' and Class Members' personal information, including the content of
22 their Internet communications, is confidential and novel.

23 195. Google knew that Plaintiffs' and Class Members trusted Google, and that their
24 personal information was disclosed to Google in confidence. As alleged and incorporated herein,
25 Google falsely represented in public statements by Google's CEO and by representations made
26 on its website that Google protected Plaintiffs and Class Members privacy, encouraged their
27 trust, and promised them that Google would not sell their personal information, all showing that
28 Google knew that their personal information was disclosed in confidence.

1 196. Google created a legal relationship with Plaintiffs and Class Members via its
2 TOS, and created a duty to protect Plaintiffs’ and Class Members’ confidential personal
3 information.

4 197. Plaintiffs and Class Members trusted Google. There was promise between Google
5 and Class Members that Google would not betray their confidence by sharing their personal
6 information without their agreement.

7 198. Google breached the trust and confidence that Plaintiffs and Class Members
8 placed in it by selling and sharing Google Customers’ personal information.

9 199. Google acted with oppression, fraud, or malice.

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

13 **NINTH CLAIM FOR RELIEF**

14 **VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT**

15 201. Google, headquartered in California, is subject to the California Invasion of
16 Privacy Act (“CIPA”), Cal. Penal Code §§ 630-638.

17 202. Google is a “person” within the meaning of § 631(a) of the Cal. Penal Code.

18 203. Google aided, agreed with, and conspired with Google RTB participants to aid
19 them in reading, and/or or using the contents or meaning of the communications being
20 exchanged connected to the Plaintiffs’ and Class Members’ personal information by employing
21 the RTB auction to sell and share Google Customer information to hundreds of Google RTB
22 participants in real-time while communications between the Google Customers and first-party
23 websites were still in transit or being sent or received within California.

24 204. Plaintiffs and Class Members did not consent to Google’s actions with Google
25 RTB participants in reading and/ or using the contents or meaning of Plaintiffs’ and Class
26 Members’ communications with websites that Plaintiffs and Class Members were directly
27 interacting with.

28 205. The cookies Google used; Plaintiffs’ and Class Members’ browsers; personal

1 computing devices; Google’s web servers; the webservers of non-Google websites from which
2 Google tracked, intercepted, shared, and sold the Plaintiffs’ and Class Members’
3 communications; and web servers of the Google RTB participants to which Google sold and
4 shared Plaintiffs’ and Class Members’ communications; and the computer code Google deployed
5 to effectuate its scheme, including but not limited to Bid Requests for each Consumer Google
6 caused to be submitted to Google RTB participants all constitute “machine[s], instrument[s], or
7 contrivance[s]” under § 631(a).

8 206. Even if the above-listed items do not constitute “machine[s], instrument[s], or
9 contrivance[s],” Google’s deliberate and purposeful efforts to facilitate its conduct comprise “any
10 other manner.”

11 207. Google’s aid to the Google RTB participants occurred in “real time.”

12 208. Google’s aid to Google RTB participants occurred while Plaintiffs’ and Class
13 Members’ communications with first-party websites were in transit or in the process of being
14 sent or received.

15 209. Google’s RTB documentation concedes that the information Google aided RTB
16 participants in reading included the “contents” and “meaning” of the Plaintiffs’ and Class
17 Members’ communications with first-party websites.

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

21 211. Plaintiffs and Class Members have a right to disgorgement and/or restitution
22 damages for the value of the stolen data because taking Plaintiffs’ and Class Members’ personal
23 information without authorization is larceny under California law

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

27 ///

28 ///

1 ///

2 **TENTH CLAIM FOR RELIEF**

3 **VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT –**
4 **UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE**

5 213. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

6 214. The Electronic Communications Privacy Act (“ECPA”) prohibits the
7 unauthorized interception of the content of any communication through the use of any device,
8 and any subsequent disclosure or use of the intercepted contents of any electronic
9 communication. 18 U.S.C. §2511.

10 215. ECPA protects both the sending and receipt of communications.

11 216. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire,
12 oral, or electronic communication is intercepted.

13 217. Google violated the interception provisions of the Electronic Communications
14 Privacy Act (“ECPA”), by either “intentionally disclosing, or endeavoring to disclose, to other
15 companies the contents of Plaintiffs’ and Class Members’ electronic communications,” 18
16 U.S.C. § 2511(1)(c); and/or by “intentionally using, or endeavoring to use, the contents of
17 Plaintiffs’ and Class Members’ electronic communications” and/or U.S.C. § 2511(1)(c).

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

22 219. Google intercepted Plaintiffs’ and Class Members’ electronic communications,
23 including:

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

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

28 c. Information that is a general summary or informs Google (and the Google
RTB participant) of the subject of communications between Plaintiffs and

1 Class members and the first-party websites.

2 220. The transmission of data between Plaintiffs and Class Members and the non-
3 Google websites with which they chose to exchange communications are "electronic
4 communications" within the meaning of 18 U.S.C. § 2510(2).

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

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

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

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

- 13 a. The cookies Google used to acquire Plaintiffs' and Class Members'
14 communications, including cookies Google sets, acquires, and discloses or
15 sells to other companies through cookie-sharing;
- 16 b. The Plaintiffs' and Class Members' browsers;
- 17 c. The Plaintiffs' and Class Members' computing devices;
- 18 d. Google's web servers;
- 19 e. The web servers of the first-party non-Google websites from which
20 Google tracked and intercepted the Plaintiffs' and Class Members'
21 communications; and
- 22 f. The computer code deployed by Google to effectuate its tracking and
23 interception of Plaintiffs' and Class Members' communications for
24 purposes of forwarding them to hundreds of Google RTB participants,
25 without authorization, including but not limited to data contained in Bid
26 Requests.

27 225. Google intentionally intercepted the contents of Plaintiffs' and Class Members'
28 electronic communications for the unauthorized purpose of selling and sharing those contents to
Google's RTB participants.

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

5 227. Google's interception of the contents of Plaintiffs' and Class Members'
6 communications was contemporaneous with their exchange with the websites to which they
7 directed their communications. As described above, the Google RTB process occurs in
8 milliseconds while the communication is still being exchanged between Plaintiffs and Class
9 Members and the website to which they directed their communications. The signal sent out to
10 Google RTB is sent simultaneously with the signal sent to the websites to which Plaintiffs' and
11 Class Members' communications were directed.

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

15 229. Google acquired the content of Plaintiffs' and Class members' electronic
16 communications with the non-Google websites to which their communications were directed
17 through the surreptitious duplication, forwarding, and re-direction of those communications to
18 Google. After intercepting the communications without authorization, Google then sold and
19 shared the contents of the intercepted communications to hundreds of Google RTB participants
20 and used the contents of the intercepted communications in furtherance of the Google RTB
21 auction.

22 230. Google's interceptions do not qualify for any exceptions under the ECPA.

23 231. As alleged throughout, Google's redirection, sale, and sharing of Plaintiffs' and
24 Class Members' personal information and the contents of their Internet communications had the
25 requisite criminal or tortious purpose for Plaintiffs' and Class Members' claims for intrusion
26 upon seclusion; publication of private facts; tortious violation of Art. I, sec. 1 of the California
27 Constitution; breach of confidence; violation of the California UCL, Cal. Bus. & Prof. Code §
28 17200; the California Invasion of Privacy Act, Cal. Penal Code § 630; the California Computer

1 Data Access and Fraud Act, Cal. Penal Code § 502; California Statutory Larceny, Cal. Penal
2 Code §§ 484 and 496; the Electronic Communications Privacy Act, 18 U.S.C. §2511; and the
3 Video Privacy Protection Act, 18 U.S.C. § 2710.

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

7 **ELEVENTH CLAIM FOR RELIEF**

8 **VIOLATION OF ECPA WIRETAP AND STORED COMMUNICATIONS ACT –**
9 **UNAUTHORIZED DISCLOSURE OF ELECTRONIC COMMUNICATIONS**

10 *(On Behalf of a Subclass Comprising All Google Customers Who Use Google Chrome)*

11 233. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

12 234. Plaintiffs are Google Customers who also use the Google Chrome web browser.

13 235. This count is brought on behalf of a subclass of all Google Customers who
14 use the Google Chrome web browser.

15 236. The Google Chrome Browser is an ECS.

16 237. The ECPA Wiretap provision of the statute provides that “a person or entity
17 providing an electronic communication service to the public shall not intentionally divulge the
18 contents of any communication (other than one to such person or entity, or an agent thereof)
19 while in transmission on that service to any person or entity other than an addressee or intended
20 recipient of such communication or an agent of such addressee or intended recipient.” 18 U.S.C.
21 § 2511(3)(a).

22 238. The ECPA Stored Communication provision provides that “a person or entity
23 providing an electronic communication service to the public shall not knowingly divulge to any
24 person or entity the contents of a communication while in electronic storage by that service.” 18
25 U.S.C. § 2702(a)(1).

26 239. Electronic Storage: The ECPA defines “electronic storage” as “any temporary,
27 intermediate storage of a wire or electronic communication incidental to the electronic
28

1 transmission thereof” and “any storage of such communication by an electronic communication
2 service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17).

3 240. Google stores Plaintiffs’ and Subclass Members’ personal information and the
4 contents of their communications in the Chrome browser and files associated with it.
5 Specifically, Google stores the content of Plaintiffs’ and Subclass Members’ Internet
6 communications within the Chrome browser in two ways:

7
8 a. For purposes of backup protection so that if the browser inadvertently
9 shuts down, Plaintiffs’ and Subclass Members’ can be presented with the option to
restore their previous communications; and

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

13 241. When a Google Customer clicks a button or hits ENTER to exchange a
14 communication with the website the Google Customer is interacting with while using the
15 Chrome browser, the content of the communication is immediately placed into storage within the
16 Chrome browser.

17 242. Google knowingly divulges the contents of Plaintiffs’ and Subclass’ members
18 communications to hundreds of different companies through the Google RTB process while such
19 communications are in electronic storage.

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

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

27
28

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

4 246. While in Transmission. Google Chrome’s divulgence of the contents of
5 Plaintiffs’ and Class Members’ communications was contemporaneous with their exchange with
6 the websites to which they directed their communications. As described above, the Google RTB
7 process occurs in milliseconds while the communication is still being exchanged between
8 Plaintiffs and Class Members and the websites to which they directed their communications.
9 That is why Google itself refers to the process as “Real-Time Bidding.” The signal sent out to
10 Google RTB is sent simultaneously with the signal sent to the websites to which Plaintiffs’ and
11 Class Members’ communications were directed.

12 247. Google Chrome is not a party to Plaintiffs’ and Class Members’ electronic
13 communications exchanged with the non-Google websites to which Plaintiffs and Class
14 Members directed their communications.

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

23 249. Exceptions to Wire Tap Do Not Apply. In addition to the exception for
24 communications directly to an ECS or an agent of an ECS, the Wiretap Act states that “[a]
25 person or entity providing electronic communication service to the public may divulge the
26 contents of any such communication”:

- 27 a. “as otherwise authorized in section 2511(2)(a) or 2517 of this title;”
28 b. “with the lawful consent of the originator or any addressee or intended

- 1 recipient of such communication;”
- 2 c. “to a person employed or authorized, or whose facilities are used, to
- 3 forward such communication to its destination;” or
- 4 d. “which were inadvertently obtained by the service provider and which
- 5 appear to pertain to the commission of a crime, if such divulgence is made to a
- 6 law enforcement agency.”

6 18 U.S.C. § 2511(3)(b).

7 250. Exceptions to Storage Do Not Apply. Section 2702(b) of the Stored
8 Communications Act provides that an electronic communication service provider “may divulge
9 the contents of a communication—”

- 10 a. “to an addressee or intended recipient of such communication or an agent
- 11 of such addressee or intended recipient;”
- 12 b. “as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;”
- 13 c. “with the lawful consent of the originator or an addressee or intended
- 14 recipient of such communication, or the subscriber in the case of remote computing
- 15 service;”
- 16 d. “to a person employed or authorized or whose facilities are used to
- 17 forward such communication to its destination;”
- 18 e. “as may be necessarily incident to the rendition of the service or to the
- 19 protection of the rights or property of the provider of that service”:
- 20 f. “to the National Center for Missing and Exploited Children, in connection
- 21 with a reported submitted thereto under section 2258A;”
- 22 g. “to law enforcement agency, if the contents (i) were inadvertently
- 23 obtained by the service provider; and (ii) appear to pertain to the
- 24 commission of a crime;”
- 25 h. “to a governmental entity, if the provider, in good faith, believes that an
- 26 emergency involving danger of death or serious physical injury to any person requires
- 27 disclosure without delay of communications relating to the emergency;” or
- 28 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.”

1 251. The hundreds of other companies to which Google divulges the content of

2 252. Plaintiffs' and Subclass Members' communications while stored in Chrome are
3 not "addressees," "intended recipients," or "agents" of any such addressees or intended recipients
4 of the Plaintiffs' and Subclass members' communications.

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

7 254. Section 2511(2)(a)(i) provides:

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

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

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

25 257. Google's divulgences of the contents of Plaintiffs' and Class Members'
26 communications on the Chrome browser to hundreds of Google RTB participants was not done
27 "with the lawful consent of the originator or any addressee or intended recipient of such
28 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, as alleged above, did Google procure the "lawful consent" of
the websites to which Plaintiffs and Subclass Members directed and exchanged communications.

1 258. Wiretap: The other companies to which Google sold, shared, and divulged
2 Plaintiffs’ and Subclass Members’ content of communications were not “person[s] employed or
3 authorized, or whose facilities are used, to forward such communication[s] to [their]
4 destination.”

5 259. Storage: The hundreds of other companies to which Google divulges the content
6 of Plaintiffs’ and Subclass Members’ communications while in Chrome storage through the RTB
7 process are not “person[s] employed or whose facilities are used to forward such communication
8 to its destination.”

9 260. The contents of Plaintiffs’ and the Subclass Members’ communications did not
10 appear to pertain to the commission of a crime, and Google Chrome did not divulge the contents
11 of their communications to a law enforcement agency.

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

16 TWELTH CLAIM FOR RELIEF

17 **VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT**

18 ***(On Behalf of a Subclass Comprising All Google Customers Who Use Google Chrome,***
19 ***Android Operating System, or Apps that Incorporate the Google Software Development Kit)***

20 262. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

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

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

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

6 265. Google is a VTSP through its Chrome browser, Android operating system, and
7 Google SDK that it provides to app developers. Google Chrome is engaged in the delivery of
8 audio-visual materials similar to prerecorded video cassette tapes by providing software through
9 which audio-visual materials are requested or obtained by Plaintiffs and Subclass Members from
10 various first-party websites accessed via the Chrome browser.

11 266. Google Android is engaged in the delivery of audio-visual materials similar to
12 prerecorded video cassette tapes by providing software through which audio-visual materials are
13 requested or obtained by Plaintiffs and Subclass Members at various first-party websites
14 accessed via a mobile device running the Android operating system.

15 267. The Google SDK is a provider of enterprise solutions for managing and
16 monetizing customers’ video that is also a Google Ad Manager certified external vendor, to
17 deliver video content to consumers, is engaged in the delivery of audio visual materials similar to
18 prerecorded video cassette tapes by providing software through which audio visual materials are
19 requested or obtained by Plaintiffs and Subclass Members at various first-party websites that
20 make use of the Google SDK to provide such audio visual materials.

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

24 269. Under the VPPA, “‘personally identifiable information’ includes information
25 which identifies a person as having requested or obtained specific video materials or services
26 from a” VTSP. 18 U.S.C. § 2710(a)(3). The VPPA definition of “‘personally identifiable
27 information” is purposefully broad and open-ended. The VPPA “prohibits ... [the disclosure of]
28 ‘personally identifiable information’ – information that links the customer or patron to particular

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

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

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

13 272. Many of the companies to which Google knowingly discloses Plaintiffs' and
14 Class Members' video purchases and viewing habits already maintain their own databases of
15 identifiers for Plaintiffs and Class Members. Facebook is one of these companies.

16 273. In addition, the identifiers Google discloses to the Google RTB participants are
17 readily capable of being used by those companies to identify specific users even in the absence
18 of a pre-existing database possessed by the recipient of Google's disclosures.

19 274. Certain types of disclosures are permitted under the VPPA. Establishing the
20 existence of such circumstances is an affirmative defense. Regardless, none exists here.

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

23 276. Disclosures were not made to law enforcement. 18 U.S.C. § 2710(b)(2)(C); *see* 18
24 U.S.C. § 2710(b)(2)(F).

25 277. Disclosures were not solely of the names and addresses of Plaintiffs and Class
26 Members where they were provided a clear and conspicuous opportunity to prohibit the
27
28

1 disclosure and the disclosure did not disclose the title, description, or subject matter of any audio
2 visual material. 18 U.S.C. § 2710(b)(2)(D).⁷⁰

3 278. Disclosures were not incident to the ordinary course of business for Google
4 Chrome, Android, or Google SDK. 18 U.S.C. § 2710(b)(2)(E).

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

10 **THIRTEENTH CLAIM FOR RELIEF**

11 **BREACH OF CONTRACT**

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

13 281. Google’s relationship with its Google Customers is governed by the Google’s
14 TOS and Privacy Policy.

15 282. Since March 31, 2020, the Google TOS incorporated by reference the document
16 titled “How our business works.”

17 283. Through these documents, Google tells Google Customers, among other things,
18 that “We don’t sell your personal information to anyone.”

19 284. Since at least May 25, 2018, the Google Privacy Policy has also told Google
20 Customers: “We don’t share information that personally identifies you with advertisers[.]”

21 285. Moreover, since at least March 1, 2012, the Privacy Policy has promised, “We do
22 not share your personal information with companies, organizations, or individuals outside of
23 Google[.]” Prior to May 2018, Google Customers who created a Google Account were required
24 to agree to both the TOS and the Privacy Policy. From May 2018 to March 31, 2020, while
25 Google Customers were required to agree to only the TOS, the Google Account creation process

26 _____
27 ⁷⁰ While the subject matter may be disclosed for the exclusive use of marketing goods and
28 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.

1 included a link to the Privacy Policy as a guide to how Google would “process your
2 information.”

3 286. Google has breached and continues to breach its contractual promise to maintain
4 the privacy of Google Customers’ personal information by selling and sharing Plaintiffs’ and
5 Class Members’ personal information through Google RTB.

6 287. As a result of Google’s breach of its contractual obligations, Google was able to
7 obtain the personal property of Plaintiffs and Class Members and cause privacy injury and other
8 consequential damages.

9 288. Plaintiffs and Class Members did not receive the benefit of the bargain for which
10 they contracted and for which they paid valuable consideration in the form of agreeing to share
11 personal information. As alleged above, this personal information has ascertainable value to be
12 proven at trial.

13 289. As a result of Google’s breach of its contractual promises, Plaintiffs and Class
14 Members are entitled to recover benefit of the bargain damages, unjust enrichment, and nominal
15 damages.

16 **FOURTEENTH CLAIM FOR RELIEF**
17 **BREACH OF THE IMPLEIED COVENANT OF**
18 **GOOD FAITH AND FAIR DEALING**

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

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

22 292. The terms of Google’s contract with Google Customers supposedly respect and
23 protect Google Customers’ privacy and promise not to sell or share their personal information.
24 Google violated these contractual promises, and frustrated the purpose of those terms by selling
25 and sharing Google Customers’ personal information.

26 293. As alleged in the Factual Section of this Complaint, Google made statements
27 concerning the supposed privacy of Google Customer personal information outside of the
28 contractual terms. By violating these extra-contractual terms and thereby acting in bad faith,

1 Google violated the implied covenant of good faith and fair dealing.

2 294. Google's failure to disclose to Plaintiffs and Class Members that it was sharing
3 and selling their personal information was unreasonable and evaded the spirit of the bargain
4 made between Google, Plaintiffs and Class Members.

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

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

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

16 **FIFTEENTH CAUSE OF ACTION**

17 **STATUTORY CIVIL LARCENY**

18 **California Penal Code Sections 484 and 496**

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

20 299. Section 496(a) prohibits the obtaining of property "in any manner constituting
21 theft." Section 484 thus defines "theft" to include obtaining property by false pretense.

22 300. Google intentionally created a platform that would operate in a manner hidden to
23 Plaintiffs whose computers were thus deceived into providing PI to Google

24 301. Google acted in a manner constituting theft and/or false pretense.

25 302. Google stole, and/or fraudulently appropriated Plaintiffs' personal information
26 without Plaintiffs' consent.

27
28

1 303. Google concealed, aided in the concealing, sold, and/or used Plaintiffs' personal
2 information that was obtained by Google for Google's commercial purposes and the financial
3 benefit of Google.

4 304. Google knew that Plaintiffs' personal was stolen because Google designed the
5 script and code that tracked Plaintiffs' personal and operated it in a manner that was concealed
6 and/or withheld from Plaintiffs.

7 305. The amount of damages is the market value of the unlawfully obtained personal
8 data.

9 **VII. PRAYER FOR RELIEF**

10 WHEREFORE, Plaintiffs respectfully request that this Court:

11 A. Award compensatory damages to Plaintiffs and the Class against Defendants for
12 all the damages resulting from Defendant's violations, in an amount to be proven at trial,
13 including interest thereon;

14 B. Award statutory damages in the amount to be proven at trial

15 C. Award Plaintiffs and the Class damages due to unjust enrichment resulting from
16 its violations identified herein, in an amount to be proven at trial, including interest thereon;

17 D. Award Plaintiffs declaratory relief finding violations of the following causes of
18 actions:

- 19 a. Google's actions violated Art. 1, § 1 of the California Constitution, Right
to Privacy;
- 20 b. Google's actions constitute publication of private information;
- 21 c. Google's actions constitute an intrusion upon seclusion
- 22 d. Google's actions violated California's Invasion of Privacy Act;
- 23 f. Plaintiffs have suffered privacy and economic harm
- 24 g. Google's actions violated the duty of confidence;
- 25 h. Google's actions violated the duty of good faith and fair dealing;
- 26 i. Google's actions violated the Electronic Communications Privacy Act;
- 27 j. Google's actions violated the Video Privacy Protection Act;
- 28 k. Google breached the contractual rights of its users

- 1 I. Google’s actions violated California’s Unfair Competition Law;
- 2 E. Injunctive relief against Google, its officers, agents, servants, employees, and
- 3 attorneys, from sharing or selling any existing account holder’s personal information without
- 4 express authorization for the sale of such information;
- 5 F. Award Plaintiffs and the Class their reasonable fees, costs and expenses incurred
- 6 in this action;
- 7 G. Award Plaintiffs and the Class punitive damages pursuant to Cal. Civ. Code §
- 8 3294(a), as Google acted with oppression, fraud, or malic and
- 9 H. Grant Plaintiffs such further relief as the Court deems appropriate.

VII. JURY TRIAL DEMAND

The Plaintiffs demand a jury trial.

Respectfully submitted,
COTCHETT, PITRE & McCARATHY, LLP

Dated: May 5, 2021

By: /s/ Nanci E. Nishimura
 NANCI E. NISHIMURA
 BRIAN DANITZ
 KARIN B. SWOPE
 NOORJAHAN RAHMAN
 BETHANY M. HILL

KNOX RICKSEN LLP
 MAISIE C. SOKOLOVE
 THOMAS E. FRAYSSE
 ITAK K. MORADI

Attorneys for Plaintiffs and the Class

Exhibit 1



April 1, 2021

Sundar Pichai
Chief Executive Officer
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

We write to seek information about your company's sharing of Americans' personal data in order to understand how that information may be obtained and exploited by foreign governments to the detriment of our national security.

Many of the ads we see on our phones, computers, and smart TVs are curated through a process called real time bidding. In the milliseconds before digital ads are displayed, an auction takes place in which hundreds of companies are able to bid for their ad to be shown. While only one company will win the auction, hundreds of firms participating receive sensitive information about the potential recipient of the ad—device identifiers and cookies, web browsing and location data, IP addresses, and unique demographic information such as age and gender. Your company operates a major advertising auction service.


Few Americans realize that some auction participants are siphoning off and storing "bidstream" data to compile exhaustive dossiers about them. In turn, these dossiers are being openly sold to anyone with a credit card, including to hedge funds, political campaigns, and even to governments.


Over the past year, multiple reports have indicated that a number of federal agencies have purchased personal data derived from mobile apps and other online services, in ways that potentially merit closer scrutiny. But the United States is not the only government with the means and interest in acquiring Americans' personal data. This information would be a goldmine for foreign intelligence services that could exploit it to inform and supercharge hacking, blackmail, and influence campaigns. As Congress debates potential federal privacy legislation, we must understand the serious national security risks posed by the unrestricted sale of Americans' data to foreign companies and governments. To that end, please provide us with answers to the following questions by May 4, 2021:

1. Please identify the specific data elements about users, their devices, the websites they are accessing, and apps they are using that you provide to auction participants.
2. Please identify each company, foreign or domestic, to whom your firm has provided bidstream data in the past three years that is not contractually prohibited from sharing, selling, or using the data for any purpose unrelated to bidding on and delivering an ad.
3. If your firm has contractual restrictions in place prohibiting the sharing, sale, or secondary use of bidstream data, please detail all efforts to audit compliance with these contractual restrictions and the results of those audits.
4. Please identify each foreign-headquartered or foreign-majority owned company to whom your firm has provided bidstream data from users in the United States and their devices in the past three years.

Thank you for your attention to this important matter.

Sincerely,


Ron Wyden
United States Senator


Bill Cassidy, M.D.
United States Senator


Kirsten Gillibrand
United States Senator


Mark R. Warner
United States Senator


Sherrod Brown
United States Senator

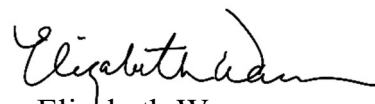

Elizabeth Warren
United States Senator

Exhibit 2

Congress of the United States

Washington, DC 20515

July 31, 2020

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons:

We write to urge the Federal Trade Commission (FTC) to investigate widespread privacy violations by companies in the advertising technology (adtech) industry that are selling private data about millions of Americans, collected without their knowledge or consent from their phones, computers, and smart TVs.

In response to complaints by privacy advocates, privacy regulators in several European countries have, over the last year, opened investigations into an adtech practice known as real time bidding (RTB). 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 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.

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. In a June 16, 2020, open letter of concern to the digital advertising industry, a group of major publishers, whose websites and apps supply the bidstream data to the RTB industry, wrote that “the current system allows for a significant data breach by companies

gaining access to the real-time bidding (RTB) infrastructure (i.e. the 'bid stream') for the sole purpose of harvesting both publisher-specific and audience-specific data.”

Americans never agreed to be tracked and have their sensitive information sold to anyone with a checkbook. Furthermore, there is no effective way to control these tools absent intervention by regulators and Congress. Technological roadblocks, such as browser privacy settings and ad blockers, are routinely circumvented by advertising companies. This outrageous privacy violation must be stopped and the companies that are trafficking in Americans' illicitly obtained private data should be shut down. Accordingly, we urge the FTC to use its authority to conduct broad industry probes under Section 6(b) of the FTC Act to determine whether adtech companies and their data broker partners have violated federal laws prohibiting unfair and deceptive business practices. The FTC should not proceed with its review of the Children's Online Privacy Protection Act (COPPA) Rule before it has completed this investigation.

We appreciate your attention to this important matter.

Sincerely,



Ron Wyden
United States Senator



Bill Cassidy, M.D.
United States Senator



Maria Cantwell
United States Senator



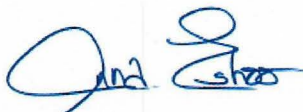
Sherrod Brown
United States Senator



Elizabeth Warren
United States Senator



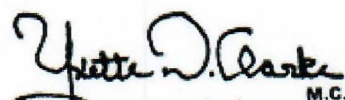
Edward J. Markey
United States Senator



Anna G. Eshoo
Member of Congress



Zoe Lofgren
Member of Congress



Yvette D. Clarke
Member of Congress



Ro Khanna
Member of Congress