

1 Lesley Weaver (Cal. Bar No.191305)
2 Angelica M. Ornelas (Cal. Bar No. 285929)
3 Joshua D. Samra (Cal. Bar No. 313050)
4 **BLEICHMAR FONTI & AULD LLP**
5 555 12th Street, Suite 1600
6 Oakland, CA 994607
7 Tel.: (415) 445-4003
8 Fax: (415) 445-4020
9 *lweaver@bfalaw.com*
10 *aornelas@bfalaw.com*
11 *jsamra@bfalaw.com*

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

8 Laurence D. King (Cal. Bar No. 206423)
9 Mario Choi (Cal. Bar No. 243409)
10 **KAPLAN FOX & KILSHEIMER LLP**
11 1999 Harrison Street, Suite 1560
12 Oakland, CA 94612
13 Tel.: (415) 772-4700
14 Fax: (415) 772-4707
15 *lking@kaplanfox.com*
16 *mchoi@kaplanfox.com*

David A. Straite (*pro hac vice* to be sought)
Aaron L. Schwartz (*pro hac vice* to be sought)
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue
New York, NY 10022
Tel.: (212) 687-1980
Fax: (212) 687-7715
dstraite@kaplanfox.com
aschwartz@kaplanfox.com

13 *Attorneys for Plaintiffs*

15 **IN THE UNITED STATES DISTRICT COURT**
16 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
17 **SAN JOSE DIVISION**

18 PATRICK CALHOUN, ELAINE
19 CRESPO, HADIYAH JACKSON and
20 CLAUDIA KINDLER, on behalf of
21 themselves and all others similarly situated,

22 Plaintiffs,

23 v.

24 GOOGLE LLC,

25 Defendant.

No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

26 **PUBLIC REDACTED VERSION WITH PLAINTIFFS’ SENSITIVE PERSONAL**
27 **INFORMATION PROVISIONALLY REDACTED PENDING MOTION TO SEAL**

TABLE OF CONTENTS

	Page
1 I. INTRODUCTION	1
2 II. JURISDICTION AND VENUE	3
3 A. Personal Jurisdiction	3
4 B. Subject Matter Jurisdiction	3
5 C. Venue	3
6 III. THE INTRADISTRICT ASSIGNMENT	4
7 IV. PARTIES	4
8 V. FACTUAL ALLEGATIONS	5
9 A. Contract Formation	5
10 B. Relevant Contract Terms.....	8
11 C. Google Improperly Collects Personal Information from Un-Synched 12 Chrome Users Without Consent and in Breach of Contract	10
13 1. Definition of Personal Information	10
14 2. An IP Address + User Agent Is Personal Information.....	12
15 3. Persistent Cookies Are Personal Information	13
16 4. X-Client Data Headers Are Personal Information	16
17 5. Browsing History is Personal Information.....	19
18 D. Chrome’s Promise Not To Share PI With Google if Not Synched Was Intended To Encourage, Not Diminish, User Engagement.....	20
19 E. How Google Instructs Chrome to Report PI to Google	23
20 F. A Sample Visit to The San Jose Mercury News Website Using Chrome – 21 Comparison Between a “Synched” Session and “Un-synched” Session.....	28
22 G. Plaintiffs’ Personal Experiences	33
23 H. Google’s Improper Collection of PI from Plaintiffs and Other Un-Synched Chrome Users is a Serious Invasion of the Privacy and is Highly Offensive.....	50
24 I. Plaintiffs’ PI Is Property Owned by the Plaintiffs and Has Economic Value.....	52
25 J. Plaintiffs Have Suffered Economic Injury.....	55
26 K. Google Has Been Unjustly Enriched	58
27 VI. CLASS ACTION ALLEGATIONS	63
28 VII. COUNTS.....	65

TABLE OF CONTENTS (cont'd.)

	Page
1	COUNT ONE WIRETAP ACT: UNAUTHORIZED INTERCEPTION OF ELECTRONIC COMMUNICATIONS..... 65
2	
3	COUNT TWO WIRETAP ACT – UNAUTHORIZED DISCLOSURES BY AN ECS 18 U.S.C. § 2510, <i>et. seq.</i> 68
4	
5	COUNT THREE STORED COMMUNICATIONS ACT – UNAUTHORIZED ACCESS TO STORED ECS COMMUNICATIONS 18 U.S.C. § 2701 70
6	
7	COUNT FOUR STORED COMMUNICATIONS ACT – UNAUTHORIZED DISCLOSURES OF STORED COMMUNICATIONS BY AN ECS 18 U.S.C. § 2701 72
8	
9	COUNT FIVE VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (“CIPA”) Cal. Penal Code §§ 631 72
10	
11	COUNT SIX INVASION OF PRIVACY 74
12	
13	COUNT SEVEN INTRUSION UPON SECLUSION..... 76
14	
15	COUNT EIGHT BREACH OF CONTRACT 77
16	
17	COUNT NINE BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING 78
18	
19	COUNT TEN QUASI-CONTRACT (RESTITUTION AND UNJUST ENRICHMENT) (IN ALTERNATIVE TO CONTRACT CLAIMS)..... 79
20	
21	COUNT ELEVEN VIOLATION OF COMPUTER FRAUD AND ABUSE ACT (“CFAA”) 18 U.S.C. §1030(g) 79
22	
23	COUNT TWELVE VIOLATION OF CALIFORNIA COMPUTER DATA ACCESS AND FRAUD ACT Cal. Penal Code § 502 80
24	
25	COUNT THIRTEEN STATUTORY LARCENY California Penal Code §§ 484 and 496..... 82
26	
27	COUNT FOURTEEN VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW (“UCL”) Cal. Bus. & Prof. Code § 17200, <i>et seq.</i> 83
28	
	COUNT FIFTEEN PUNITIVE DAMAGES Cal. Civ. Code § 3294..... 85
	COUNT SIXTEEN DECLARATORY RELIEF 28 U.S.C. § 2201(a)..... 85
	VIII. PRAYER FOR RELIEF..... 86
	IX. JURY TRIAL DEMAND 87

TABLE OF EXHIBITS

EX.	DOCUMENT DESCRIPTION
1	Chart of Documents Constituting the Relevant Contract by Date
2	Google Terms of Service dated April 14, 2014
3	Google Terms of Service dated Oct. 25, 2017
4	Google Terms of Service dated March 31, 2020
5	Chrome Terms of Service dated Aug. 12, 2010
6	Google Chrome and Chrome OS Additional Terms of Service dated March 31, 2020
7	Google Privacy Policy dated June 28, 2016
8	Google Privacy Policy dated Aug. 29, 2016
9	Google Privacy Policy dated March 1, 2017
10	Google Privacy Policy dated April 17, 2017
11	Google Privacy Policy dated Oct. 2, 2017
12	Google Privacy Policy dated Dec. 18, 2017
13	Google Privacy Policy dated May 25, 2018
14	Google Privacy Policy dated Jan. 22, 2019
15	Google Privacy Policy dated Oct. 15, 2019
16	Google Privacy Policy dated Dec. 19, 2019
17	Chrome Privacy Notice dated June 21, 2016
18	Chrome Privacy Notice dated August 30, 2016
19	Chrome Privacy Notice dated Oct. 11, 2016
20	Chrome Privacy Notice dated Nov. 30, 2016
21	Chrome Privacy Notice dated Jan. 24, 2017
22	Chrome Privacy Notice dated March 7, 2017
23	Chrome Privacy Notice dated April 25, 2017

TABLE OF EXHIBITS

EX.	DOCUMENT DESCRIPTION
24	Chrome Privacy Notice dated March 6, 2018
25	Chrome Privacy Notice dated Sept. 24, 2018
26	Chrome Privacy Notice dated Oct. 24, 2018
27	Chrome Privacy Notice dated Dec. 4, 2018
28	Chrome Privacy Notice dated Jan. 30, 2019
29	Chrome Privacy Notice dated Mar. 12, 2019
30	Chrome Privacy Notice dated Oct. 31, 2019
31	Chrome Privacy Notice dated Dec. 10, 2019
32	Chrome Privacy Notice dated March 17, 2020
33	Chrome Privacy Notice dated May 20, 2020

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

1 **I. INTRODUCTION**

2 1. This is a nationwide data privacy class action brought by and on behalf of Google
3 Chrome users who chose not to “Sync” their browsers with their Google accounts while browsing
4 the web (“Un-Synched Chrome Users”) from July 27, 2016 to the present (the “Relevant Period”).

5 2. Google expressly promises Chrome users that they “don’t need to provide any
6 personal information to use Chrome” and that “[t]he personal information that Chrome stores won’t
7 be sent to Google unless you choose to store that data in your Google Account by turning on
8 sync[.]”

9 3. Despite these express and binding promises, Google intentionally and unlawfully
10 causes Chrome to record and send users’ personal information to Google *regardless of whether a*
11 *user elects to Sync or even has a Google account.*

12 4. Examples of personal data improperly created and sent to Google by Chrome
13 include:

- 14 a. IP addresses linked to user agents;
- 15 b. Unique, persistent cookie identifiers including the Client ID;
- 16 c. Unique browser identifiers called X-Client Data Headers; and
- 17 d. Browsing history.

18 5. This Complaint provides specific examples of the personal data flow that Chrome
19 sent from Plaintiffs’ devices as they used Chrome while not Synched, demonstrating that Chrome
20 secretly sends personal information to Google even when a Chrome user does not Sync.

21 6. Google’s contract with Chrome users designates California law, and consistent with
22 California law, defines “Personal Information” as “information that you provide to us which
23 personally identifies you . . . *or other data that can be reasonably linked to such information by*
24 *Google, such as information we associate with your Google Account.*”

25 7. Each category of data identified above is “personal information” because it either
26 personally identifies the user or can be reasonably linked to such information. Furthermore, Google
27 affirmatively discloses that it associates data gathered from Chrome with users. Google has
28 therefore breached its contract with Un-Synched Chrome Users.

1 8. The improperly collected web browsing history also consists of electronic
2 communications that contain content protected by California and federal wiretap laws. Google
3 collects the content contemporaneously with the communications; Google does not obtain consent
4 from Un-Synched Chrome Users to intercept these communications; and Google is not a party to
5 them. Google is thus violating the federal Electronic Communications Privacy Act and analogue
6 California statutes.

7 9. Google's actions are a serious violation of user privacy. Google tracking code is
8 found on websites accounting for more than half of all internet traffic and Chrome is the dominant
9 web browser (used on a majority of desktop computers in the United States), giving Google
10 unprecedented power to surveil the lives of more than half of the online country in real time. And
11 because some of Google's third-party tracking cookies are disguised as first-party cookies to
12 facilitate cookie synching, Google is misrepresenting its privacy practices in ways that have been
13 successfully challenged by the FTC in the past.¹

14 10. Google's extensive network of affiliates—Google Sites, Google Apps, Google
15 Account, Google Drive, Google AdWords—as well as its business partnerships means that sharing
16 information with Google feeds it into a massive interconnected database of surveillance material.
17 Google's surveillance of the Plaintiffs and other Un-Synched Chrome Users directly contradicts its
18 promises to honor users' choice not to share data. This is a serious and irreversible invasion of
19 privacy that is invisible to Google users.

20 11. Google's actions also constitute rank theft. Plaintiffs' PI is a form of property
21 recognized under California law and has economic value in the marketplace. Taking Plaintiffs' PI
22 from their computers without consent is larceny; any profits earned on the PI are unjustly earned at
23 the expense of Plaintiffs and must be disgorged. Had Google been transparent about its level of
24 surveillance, user engagement—a key metric for Google's sales—would have decreased.

25 12. Google's actions also constitute unlawful computer intrusion under California and
26 federal law. Google introduced computer code into Plaintiffs' computers and caused damage

27 ¹ *United States v. Google, Inc.*, 12-cv-4177-SI (N.D. Cal.), complaint dated Aug. 8, 2012, at ¶ 46-
28 47.

1 without authorization by turning the computers into surveillance machines that reported Plaintiffs’
2 personal information, including private web browsing, to Google, in real time.

3 13. Plaintiffs and the other Un-Synched Chrome Users have suffered privacy harm and
4 economic harm as a result of Google’s wrongful acts. Plaintiffs therefore bring contract, statutory,
5 common law and equitable claims against Google for money damages, restitution, disgorgement,
6 punitive damages and injunctive relief.

7 **II. JURISDICTION AND VENUE**

8 **A. Personal Jurisdiction**

9 14. This Court has personal jurisdiction over Defendant because Defendant is
10 headquartered in this District. Google also concedes personal jurisdiction in the current and prior
11 general Google Terms of Service. *See* Exhibits 2 through 4.

12 **B. Subject Matter Jurisdiction**

13 15. This Court has subject matter jurisdiction over the federal claims in this action,
14 namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the “Wiretap Act”), the Stored Communication
15 Act, 18 U.S.C. § 2701 (“SCA”), the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the
16 “CFAA”) and request for Declaratory Relief under 18 U.S.C. § 2201, pursuant to 28 U.S.C. § 1331.

17 16. This Court also has subject matter jurisdiction over this entire action pursuant to the
18 Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), because this is a class action in which
19 the amount in controversy exceeds \$5,000,000, and at least one member of the class is a citizen of
20 a state other than California or Delaware.

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

24 **C. Venue**

25 18. Venue is proper in this District because the Defendant is headquartered in this
26 District. In addition, in the current Google general Terms of Service and prior versions, Google
27 purports to bind Plaintiffs to bring disputes in this District. *See* Exhibits 2 through 4.

28

1 **III. THE INTRADISTRICT ASSIGNMENT**

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

5 **IV. PARTIES**

6 20. Plaintiff Patrick Calhoun is an adult domiciled in Florida. Plaintiff has used the
7 Chrome browser on his personal laptop for numerous activities, including exchanging
8 communications with state government agencies [REDACTED].
9 Plaintiff has also routinely used the Chrome browser to exchange communications about news,
10 politics, and more. Plaintiff has not enabled Sync with his Google accounts on his personal laptop
11 and never consented to Chrome sharing his Personal Information, including the contents of his
12 Internet communications, with Google. Despite his lack of consent and expressly promising
13 otherwise, Chrome shared Calhoun's personal information with Google, including the content of
14 his communications. Plaintiff has temporarily stopped using Chrome but wishes to use it again
15 once Google stops tracking un-synched users.

16 21. Plaintiff Elaine Crespo is an adult domiciled in Florida. Plaintiff has used the
17 Chrome browser on her personal laptop for numerous activities, including exchanging
18 communications relating to banking, her children's education, and for her employment. Plaintiff
19 has not enabled Sync with her Google accounts on her personal laptop and never consented to
20 Chrome share her personal information, including the contents of her Internet communications,
21 with Google. Despite her lack of consent and expressly promising otherwise, Chrome shared
22 Crespo's personal information with Google, including the contents of her communications.
23 Plaintiff has temporarily stopped using Chrome but wishes to use it again once Google stops
24 tracking un-synched users.

25 22. Plaintiff Hadiyah Jackson is an adult domiciled in Pennsylvania. Plaintiff and her
26 family have used the Chrome browser on her personal laptop for numerous activities, including
27 exchanging communications with state government agencies regarding an [REDACTED]
28 [REDACTED] Plaintiff has not enabled Sync with her Google accounts on her personal

1 laptops and never consented to Chrome sharing her Personal Information, including the contents of
2 her Internet communications, with Google. Despite her lack of consent and expressly promising
3 otherwise, Chrome shared Jackson’s personal information with Google, including the content of
4 her communications. Plaintiff has temporarily stopped using Chrome but wishes to use it again
5 once Google stops tracking un-synched users.

6 23. Plaintiff Claudia Kindler is an adult domiciled in California. Plaintiff has used the
7 Chrome browser on her personal laptop for numerous activities, including exchanging
8 communications with her banks, healthcare providers, and continuing education providers for her
9 employment. Kindler has also routinely used the Chrome browser to exchange communications
10 about politics and more. Plaintiff has not enabled Sync with her Google accounts on her personal
11 laptops and never consented to Chrome sharing her Personal Information, including the contents of
12 her Internet communications, with Google. Despite her lack of consent and expressly promising
13 otherwise, Chrome shared Kindler’s personal information with Google, including the content of
14 her communications. Plaintiff has temporarily stopped using Chrome but wishes to use it again
15 once Google stops tracking un-synched users.

16 24. Google LLC (“Google”) is a Delaware Limited Liability Company based at
17 1600 Amphitheatre Way, Mountain View, California, whose memberships interests are entirely
18 held by its parent holding company, Alphabet, Inc. (“Alphabet”), headquartered at the same
19 address. Alphabet trades under the stock trading symbols GOOG and GOOGL. Alphabet generates
20 revenues primarily by delivered targeted online advertising through the Google LLC subsidiary.
21 All operations relevant to this complaint are run by Google LLC.

22 25. In this Complaint, “Google” refers to Google LLC unless otherwise specified

23 **V. FACTUAL ALLEGATIONS**

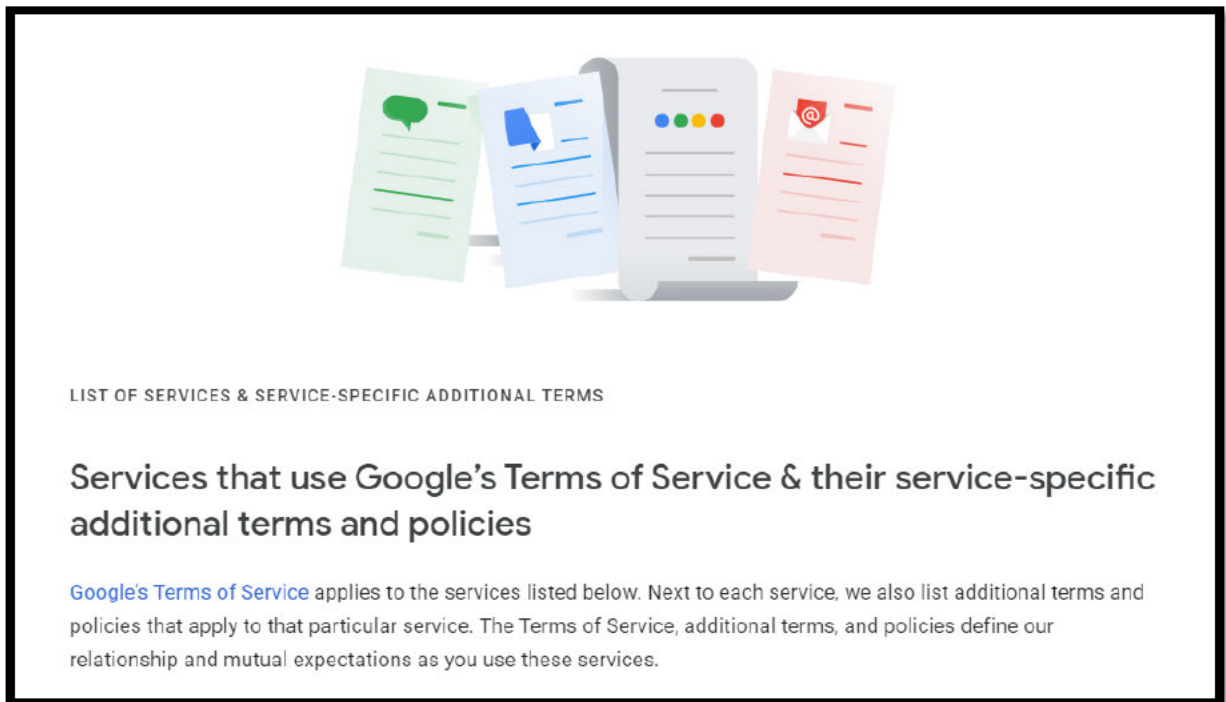
24 **A. Contract Formation**

25 26. The current contract governing the relationship between Google and Chrome with
26 respect to Chrome consists of three documents: the Google general Terms of Service dated
27 March 31, 2020 (Exhibit 4) (“General TOS”); the Google Chrome and Chrome OS Additional
28

1 Terms of Service dated March 31, 2020 (Exhibit 6) (“Chrome TOS”); and the Chrome Privacy
2 Notice dated May 20, 2020 (Exhibit 33) (“Chrome Privacy Notice”).²

3 27. These documents are revised frequently, see chart in Exhibit 1, but the core contract
4 terms relevant to this Action are the same throughout the Relevant Period.

5 28. The General TOS incorporates by reference and hyperlinks to “service-specific
6 additional terms and policies” as illustrated below and in Exhibit 4. The General TOS provides that
7 certain identified services are governed by the General TOS as well as “additional terms and
8 policies that apply to that particular service.” It continues, “[t]he Terms of Service, *additional terms*
9 *and policies* define our relationship and mutual expectations as you use these services”:



22

23

24

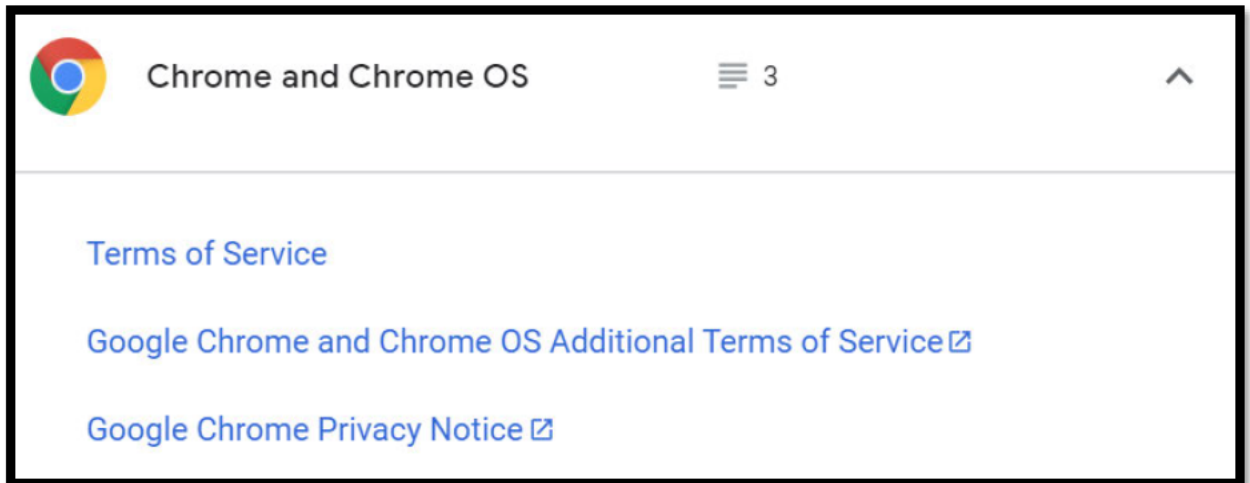
25

26

27 ² Prior to March 31, 2020, the contract also included a fourth document, the Google general Privacy Policy (Exhibits 7 through 16).

28

1 29. The General TOS then identifies Chrome as a “service” and identifies (and
2 hyperlinks to) three documents that govern the use of Chrome and together constitute the contract:



11

12 30. The General TOS contains 15 separate references and links to the “service-specific
13 additional terms and policies.” Every time this term is referenced, a hyperlink is included that
14 incorporates and links users to the “List of services & service-specific additional terms.”

15 31. Prior to March 31, 2020, the Chrome TOS itself also expressly incorporated the
16 Chrome Privacy Notice as a part of the contract. The Chrome TOS dated Aug. 12, 2010 states that
17 users’ “agreement with Google” includes “the terms set forth” in the General TOS as well as
18 “Google Chrome Additional Terms of Service and terms of any Legal Notices applicable to the
19 Services.” *See* Ex. 5.

20 32. The Chrome TOS further states that “[f]or more information about Google’s data
21 protection practices, please read Google’s privacy policy at <http://www.google.com/privacy.html>
22 and at <https://www.google.com/intl/en/chrome/privacy/>.” These two URLs link to the web pages
23 where the Google Privacy Policy and the Chrome Privacy Notice were publicly available.

24 33. Finally, the General TOS specifies that “service-specific additional terms” govern
25 where there is a conflict with the General TOS:

26

27

28

If these terms conflict with the [service-specific additional terms](#), the additional terms will govern for that service.

1 34. At all times during the Relevant Period, therefore, the Chrome Privacy Notice was
2 a part of the contract between Plaintiffs and Google and supersedes any conflicting term in the
3 General TOS.

4 **B. Relevant Contract Terms**

5 35. The Chrome Privacy Notice represents that it is the place where users can “Learn to
6 control the information that’s collected, stored, and shared when you use the Google Chrome
7 browser[.]” *See* Ex. 33.

8 36. In the Chrome Privacy Notice, Google promised that Chrome would not send any
9 Personal Information to Google unless the Chrome User affirmatively chose to Sync the browser
10 with his or her Google Account.

11 37. Specifically, from June 2016 to present, all versions of the Chrome Privacy Notice
12 have promised that “You don’t need to provide any personal information to use Chrome.” *See*
13 Exs. 17-33.

14 38. In addition, all versions of the Chrome Privacy Notice have promised that Chrome
15 will not send Personal Information to Google unless the Chrome user chooses to Sync the browser
16 with his or her Google account:

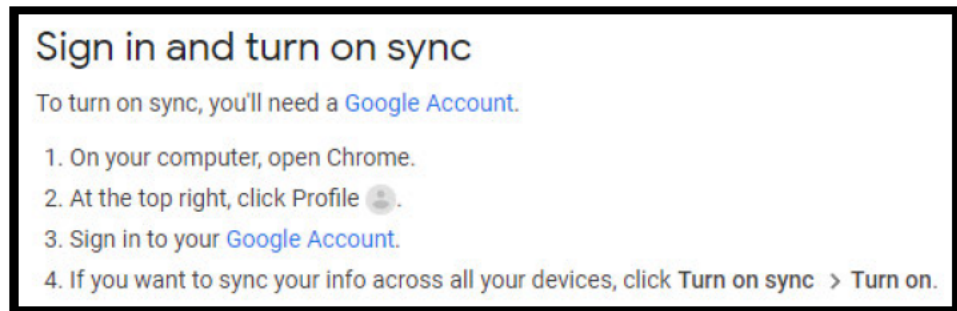
17 a. From January 30, 2019 to the present, Google promises that “the personal
18 information that Chrome stores won’t be sent to Google unless you choose to
19 store that data in your Google Account by turning on sync.” *See* Exs. 28-33.

20 b. From September 24, 2018 to January 30, 2019, Google promised that “the
21 personal information that Chrome stores won’t be sent to Google unless you
22 choose to store that data in your Google Account by turning on Chrome
23 sync.” *See* Exs. 25-27.

24 c. Prior to September 24, 2018, the Chrome Privacy Notice promised “The
25 personal information that Chrome stores won’t be sent to Google unless you
26 choose to store that data in your Google Account by signing in to Chrome.
27 Signing in enables Chrome’s synchronization feature.” *See* Exs. 17-24.
28

1 39. The Chrome Privacy Notice has always promised that Sync will only be enabled by
2 your choice to take an affirmative act. Syncing has never been a default setting during the Relevant
3 Period. For example, from September 24, 2018 to present, a Chrome user had to take the follow
4 affirmative steps to enable Sync:

- 5 a. On a desktop,³ the user can enable Sync by taking “open[ing] Chrome,
6 clicking the “Profile” icon at the top right, signing in to the user’s “Google
7 Account,” clicking “Turn on sync” and then “Turn on.” An example is shown
8 here:



- 14 b. On a mobile device, a user downloads the Chrome app, clicks the “...” to the
15 right of the address bar, clicks “Settings,” then clicks “Sign in to Chrome,”
16 then “Tap the account [the user] want[s] to use,” tap “Continue,” and then tap
17 “OK, Got it.” An example of these steps for Android users is shown below:⁴
18

19

20

21

22

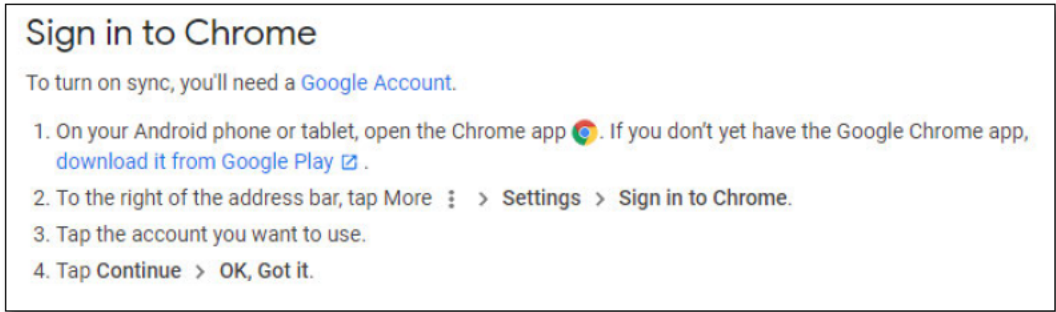
23

24

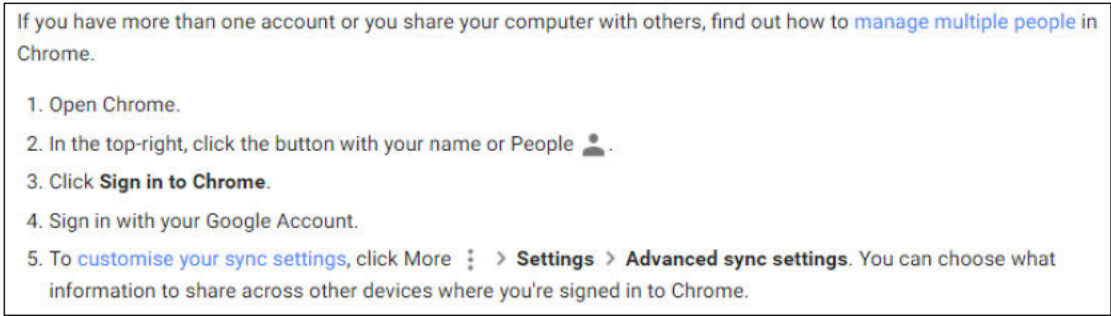
25 ³ *Turning sync on and off in Chrome*, Google Chrome Help, <https://support.google.com/chrome/answer/185277?co=GENIE.Platform%3DDesktop&oco=1>
26 (last visited July 19, 2020).

27 ⁴ *Turn sync on and off in Chrome*, Google Chrome Help, <https://support.google.com/chrome/answer/185277?co=GENIE.Platform%3DAndroid&oco=1>
28 (last visited July 19, 2020).

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



40. Prior to September 24, 2018, the process was different but still required at least four affirmative steps to enable Chrome synchronization through the Chrome sign-in feature.⁵



41. On mobile devices, users had to take similar steps to enable Chrome.⁶

C. Google Improperly Collects Personal Information from Un-Synched Chrome Users Without Consent and in Breach of Contract

1. Definition of Personal Information

42. The contract designates California law as the governing law.

43. California law defines “Personal Information” as, and it is used in this Complaint to mean: “information that identifies, relates to, describes, *is reasonably capable of being associated with*, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

⁵ Sign in to Chrome, Chrome Help, <https://web.archive.org/web/20170411045120/https://support.google.com/chrome/answer/185277> (archived on Apr. 11, 2017).

⁶ See e.g., Travis Boylss, *How to Sync Bookmarks on Chrome on iPhone or iPad*, WikiHow (Dec. 24, 2017), <https://www.wikihow.tech/Sync-Bookmarks-on-Chrome-on-iPhone-or-iPad>.

1 Personal information includes, but is not limited to, the following if it identifies, relates to,
2 describes, is reasonably capable of being associated with, or could be reasonably linked, directly
3 or indirectly, with a particular consumer or household:

- 4 a. Identifiers such as a real name, alias, postal address, unique personal
5 identifier, online identifier, internet protocol address, email address, account
6 name, social security number, driver's license number, passport number, or
7 other similar identifiers;
- 8 b. Any categories of personal information described in subdivision (e) of
9 Section 1798.80.
- 10 c. Characteristics of protected classifications under California or federal law;
- 11 d. Commercial information, including records of personal property, products
12 or services purchased, obtained, or considered, or other purchasing or
13 consuming histories or tendencies;
- 14 e. Biometric information;
- 15 f. Internet or other electronic network activity information, including, but not
16 limited to, browsing history, search history, and information regarding a
17 consumer's interaction with an internet website, application, or
18 advertisement;
- 19 g. Geolocation data;
- 20 h. Audio, electronic, visual, thermal, olfactory, or similar information;
- 21 i. Professional or employment-related information;
- 22 j. Education information, defined as information that is not publicly available
23 personally identifiable information as defined in the Family Educational
24 Rights and Privacy Act (20 U.S.C. § 1232(g); 34 C.F.R. Part 99);
- 25 k. Inferences drawn from any of the information identified in this subdivision
26 to create a profile about a consumer reflecting the consumer's preferences,
27 characteristics, psychological trends, predispositions, behavior, attitudes,
28 intelligence, abilities, and aptitudes.”

1 Cal. Civ. Code § 1798.140(o)(1) (emphasis added).

2 44. The Google general Privacy Policy also expressly tracks the California statutory
3 definition of “personal information,” defining it as “information that you provide to us which
4 personally identifies you, such as your name, email address, or billing information, *or other data*
5 *that can be reasonably linked to such information by Google*, such as information we associate
6 with your Google Account.” *See* Ex. 16 (emphasis added).

7 45. The following data qualifies as personal information when Google code instructs
8 the Google Chrome browser to report it to Google:

- 9 a. IP addresses linked to user agent;
- 10 b. Session and Persistent cookie identifiers;
- 11 c. X-client-data headers; and
- 12 e. Browsing history and information regarding a consumer’s interaction with
13 an Internet website.

14 46. Google is reasonably capable of linking IP addresses (including those linked to user
15 agent), persistent cookie identifiers, X-client-data headers, and web browsing history and
16 information regarding a consumer’s interaction with an Internet website, and, in fact, does link such
17 information with individual consumers and their devices.

18 **2. An IP Address + User Agent Is Personal Information**

19 47. An IP address is a number that identifies a computer connected to the Internet.

20 48. IP addresses are used to identify and route communications on the Internet.

21 49. An IP address is not the same thing as a URL.

22 50. IP addresses of individual Internet users are used by Internet service providers,
23 websites, and tracking companies to facilitate and track Internet communications.

24 51. Google tracks IP addresses associated with specific Internet users.

25 52. Google is capable of and does in fact associate specific users with specific IP
26 addresses. For example, when a user signs into a Gmail account, Google associates the personal
27 information connected with that email account to the IP address in question.

28

1 53. Even if a specific IP address is shared by multiple devices on a single network,
2 Google is capable of and does, in fact, associate specific users with specific IP addresses. Google
3 does so through its use of other identifiers tied to an IP address, including User-Agent, which is a
4 list of properties identifying a device within a network.

5 54. Because Google collects the IP Address and user agent information together, Google
6 can identify a user's individual device even if more than one device shares the same IP Address.

7 **3. Persistent Cookies Are Personal Information**

8 55. A cookie is a small text file that a web-server can place on a person's web browser
9 and computing device when that person's web browser interacts with the website server.

10 56. Cookies can perform different functions. Eventually, some cookies were designed
11 to acquire and record an individual Internet user's communications and activities on websites across
12 the Internet.

13 57. Cookies are designed to and, in fact, do operate as a means of identification for
14 Internet users.

15 58. In general, cookies are categorized by (1) duration and (2) party.

16 59. There are two types of cookies classified by duration:

17 a. "Session cookies" are placed on a user's computing device only while the
18 user is navigating the website that placed and accesses the cookie during a
19 single communication session. The user's web browser deletes session
20 cookies when the user closes the browser.

21 b. "Persistent cookies" are designed to survive beyond a single Internet-
22 browsing session. The party creating the persistent cookie determines its
23 lifespan. As a result, a persistent cookie can acquire and record a user's
24 Internet communications for years and over dozens, hundreds, or thousands
25 of websites. Persistent cookies are sometimes called "tracking cookies."

26 60. Cookies are also classified by the party that uses the collected data:

27 a. "First-party cookies" are set on a user's device by the website with which
28 the user is exchanging communications. For example, Google uses cookies

1 on users' browsers when users' directly visit Google properties such as
 2 Gmail. First-party cookies can be helpful to the user, server, and/or website
 3 to assist with security, log-in, and functionality.

- 4 b. "Third-party cookies" are set on a user's device by website servers other than
 5 the website or server with which the user is exchanging communications.
 6 For example, the same Gmail user might also have cookies on their Chrome
 7 browser that are set by Google's other services such as Google Ads or
 8 Google Doubleclick. Unlike first-party cookies, third-party cookies are not
 9 typically helpful to the user. Instead, third-party cookies are typically used
 10 for data collection, behavioral profiling, and targeted advertising.

11 61. Google uses several cookies to identify specific Internet users and their devices,
 12 including the following:

13 14 15 16	SID HSID	These cookies contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time. They are unique and persistent on a user's device for two years or more.
17 18 19	_Secure-SSID _Secure-HSID	These cookies are "secure" cookies that Google sets and accesses when a user signs into a Gmail account and does not formally log-off even after the user has left the Gmail website. They are unique and persistent on a user's device for six months or more.
20 21 22	NID	The NID cookie contains a unique ID Google uses to remember user preferences and other information, including, for example, how many search results they wish to have shown per page and whether they have Google's SafeSearch filter turned on. NID is also used to help customize ads on Google properties, like Google search. NID is unique and persistent on a user's device for two years or more.
23 24 25	SSID APISID SAPISID	These cookies are unique and persistent on a user's device for two years or more. Google does not publicly state their purpose.
26 27 28	_Secure-3PSID _Secure-APISID _Secure-3PAPISID	These cookies are "secure" cookies that Google sets and accesses when a user signs into a Gmail account and does not formally log-off even after the user has left the Gmail website.
	IDE	Google uses the IDE cookie for advertising. It is unique and persistent on a user's device for two years or more.
	DSID	Google also uses the DSID cookie for advertising. It is unique and persistent on a user's device for two years or more.

62. Google also engages in a controversial practice known as "cookie synching" which further allows Google to associate cookies with specific individuals. With cookie synching, first-

1 party cookies are set by websites with which users are directly interacting, but then those first-party
2 websites also pass that cookie values along to Google Analytics, where Google takes the personal
3 information it has about the user's particular browser and links the Google Analytics first-party
4 cookie information to Google's own third-party cookies and the user's browsing.

5 63. Based on an Internet security policy known as the same-origin policy, web-browsers
6 are supposed to prevent different entities from accessing each other's cookies. For example, at the
7 San Jose Mercury News website, Google would be prevented from accessing the new site's "first-
8 party" cookie values. And vice-versa, the San Jose Mercury News would be prevented from
9 accessing Google.com's third-party cookie values.

10 64. However, Javascript source code running on a webpage can bypass the same origin
11 policy protections by sending a putative 'first-party' cookie value in a tracking pixel to a third-party
12 entity. This technique is known in the Internet advertising business as "cookie synching."

13 65. Cookie synching allows cooperating websites to learn each other's cookie
14 identification numbers for the same user. Once the cookie synching operation is complete, the two
15 websites exchange information that they have collected and hold about a user, further making these
16 cookies "Personal Information."

17 66. The Google cookie-synching cookie is called "*cid*," which is short for the "Client
18 ID" that Google assigns to a specific user. As Google admits in its Google Analytics documentation
19 for web-developers, the *cid* cookie is personal information:

20 In order for Google Analytics to determine that two distinct hits
21 belong to the same user, a unique identifier, associated with that
22 particular user, must be sent with each hit. The analytics.js library
23 accomplishes this via the Client ID field, a unique, randomly
24 generated string that gets stored in the browser's cookies, *so
25 subsequent visits to the same site can be associated with the same
26 user.*⁷

27 67. Chrome shares the Client ID value with Google regardless of a user's Sync status or
28 log-in status with Google Ads, Google Doubleclick, and Google Analytics. Even worse, Chrome
29 shares Google's *cid* cookie value with Google even when third-party cookies are blocked.

⁷ <https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id>.

1 Disguising third-party tracking cookies as first-party cookies is a deceptive privacy practice already
2 successfully challenged by the FTC when Google attempted it in 2011. *United States v. Google, Inc.*,
3 12-cv-4177-SI (N.D. Cal.), complaint dated Aug. 8, 2012, at ¶ 46-47.

4 68. In addition to sending Google the “CID” cookie value, Chrome also sends cookie-
5 synched values for Google cookies named `_gads ID`, `_gcl_au/auiddc`, and `_gid` to Google.

6 **4. X-Client Data Headers Are Personal Information**

7 69. The x-client-data header is an identifier that when combined with IP address and
8 user-agent, uniquely identifies every individual download version of the Chrome browser.

9 70. The x-client-data identifier is sent from Chrome to Google every time users
10 exchange an Internet communication, including when users log-in to their specific Google
11 accounts, use Google services such as Google search or Google maps, and when Chrome users are
12 neither signed-in to their Google accounts nor using any Google service.

13 71. Chrome has created and sent the x-client-data identifier to Google with every
14 communication users exchange since at least March 6, 2018.

15 72. The x-client-identifier is not disclosed in any term of service or privacy policy
16 operative at any time.

17 73. It is also not hyperlinked to any of these policies and the average, reasonable
18 Chrome user had no reason to know of its existence.

19 74. Google first publicly admitted to the existence of the x-client-data identifier to the
20 tech community in a document called the Chrome Privacy White Paper, published on March 6,
21 2018. The White Paper assisted developers on the “read” side—or surveillance side—with
22 developing products that could extract this information and further pair it with existing data.

23 75. The White Paper is authored by Google and makes several admissions relevant to
24 this action, as well as furthering the impression that Chrome was not sending personal information
25 to Google in violation of its express promises.

26 76. The White Paper begins by stating, “This document describes the features in
27 Chrome that communicate with Google, as well as with third-party services (for example, if you've
28 changed your default search engine).”

1 77. Despite claiming the it would “describe[] the features in Chrome that communicate
2 with Google[,]” the White Paper does not disclose that Chrome sends users’ personal information
3 to Google regardless of whether users are logged-in to their Google Sync account or not.

4 78. Initially, the White Paper falsely represented that the x-client data identifier, which
5 it called a “Chrome-Variations header” did “not contain any personally identifiable information
6 and will only describe the state of the installation of Chrome itself, including active variations, as
7 well as server-side experiments that may affect the installation.”⁸

8 79. However, on September 24, 2018, researcher and technologist Vincent Toubiana
9 with ARCEP (a French Telecom regulator), who runs the blog www.unsearcher.org, took notice of
10 X-client-data. What he learned alarmed him:

11 **“The x-client-data header**

12 This is probably the most problematic header and I did not see it
13 mention anywhere else than in the whitepaper. *Most users are not*
14 *aware of it but this header is sent with every request sent to Google*
15 *services* (and only Google services) to do A/B testing. Google
16 services include most Google domains, including Doubleclick. Even
17 when Google is a third party, the header is sent. Because it’s a header
18 and not a cookie, it is sent even when you block cookies.

19

20 *So not only does this header may [sic] have some privacy*
21 *implications, it makes the browser not neutral as it gives more data*
22 *to Google services.*

23 . . .

24 **Conclusion**

25 . . . by using custom headers, Google is less and less dependent on
26 third party cookies. *I would not be surprised if Chrome started to*
27 *block third party cookies.* Actually this may be in Google financial
28 interest to do that.⁹

26 ⁸ <https://web.archive.org/web/20180505082442/https://www.google.com/chrome/privacy/whitepaper.html>

27 ⁹ <https://unsearcher.org/more-on-chrome-updates-and-headers>

1 80. On January 14, 2020, Google announced that Chrome would be phasing out the use
2 of third-party cookies over two years. Google cynically claimed that its decision was driven by the
3 fact that “[u]sers are demanding greater privacy—including transparency, choice, and control over
4 how their data is used.”¹⁰ Left unsaid was the fact that *Chrome’s x-client header can now uniquely*
5 *identify a majority of web-browsers in the United States, and Google does not need tracking*
6 *cookies anymore*. Now that Google controls both the online ad market and the browser market
7 simultaneously, blocking third-party cookies simply blocks competing trackers, while Google has
8 a method to continue back-door tracking through the unique browser identifier created and
9 disclosed by its browser without any notification to users.

10 81. In addition to uniquely identifying Plaintiffs’ browsers, Google also uses the x-
11 client-identifier to track them across other Google services. For example, on February 4, 2020,
12 Arnaud Granal, the developer of the Kiwi Browser (a Chromium-based alternative browser for
13 Android) discovered and disclosed that x-client-data is “a unique ID to track a specific Chrome
14 instance across all Google properties,” including, in his example, YouTube and Doubleclick.¹¹

15 82. Similarly, Kyle Bradshaw at www.9to5google.com explained the x-client-data
16 identifier “is sent to those Google servers regardless of whether you’re logged in with your Google
17 Account or not, which could theoretically tie your logged-out browsing back to your Google
18 Account.”¹²

19 83. Bradshaw further explained, “Putting it all together, the accusation being leveled
20 against Google by the tech community is that the company is making it harder for competing ad
21 networks and other third-parties to track your browsing while their own purported tracking method
22 is able to continue uninhibited.” Regardless of the impact on competitors, the impact on Plaintiffs
23 and the Class is significant—they cannot escape this new and even more secretive form of
24 surveillance.

25
26 ¹⁰ <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>

27 ¹¹ <https://github.com/w3ctag/design-reviews/issues/467#issuecomment-581944600>

28 ¹² <https://9to5google.com/2020/02/06/google-chrome-x-client-data-tracking/>

1 84. Following the revelations above, Google quietly amended its White Paper to remove
 2 its false representations about the x-client header. For example, on March 12, 2020, in an article
 3 called “Google Backpedals on Claim that X-Client-Data Doesn’t Contain PI Information,” it was
 4 reported by VPN Overview:

5 Originally the information about the X-Client-Data header in the
 6 whitepaper was as follows: “A list of field trials that are currently
 7 active on your installation of Chrome will be included in all requests
 8 sent to Google. This Chrome variations header (X-Client-Data) will
 9 not contain any personally identifiable information, and will only
 10 describe the state of the installation of Chrome itself, including active
 11 variations, as well as server-side experiments that may affect the
 12 installation.” *In the latest version of the whitepaper, the text stating
 13 that the X-Client-Data header doesn’t contain any PI information
 14 has been removed.*¹³

15 85. VPN Overview further explained:

16 The fact that Google may be tracking users through the X-Client-
 17 Data header, is in itself of concern. However, it is not the most
 18 important issue here. Google probably has other means for tracking
 19 users. *Of greater concern is the fact that Google did not disclose
 20 what it was using the header for. Google is tracking users without
 21 their knowledge, which is a violation of users’ privacy.
 22 Furthermore, the original description of the header’s use was
 23 incredibly inaccurate and likely to have been in breach of legal
 24 compliance requirements.*

25 86. As of the date of filing, Google still has not fixed the Chrome Privacy Notice, the
 26 Google general Terms of Use, or the Google Privacy Policy to accurately disclose the X-Client-
 27 Data identifier and its uses.

28 5. Browsing History is Personal Information

87. Browsing history consists of a record of a communication or communications that
 a user exchanges on the Internet and includes both the content of the communication or
 communications and data associated with it, such as the time of the communication or
 communications.

88. California law defines “personal information” to include browsing history,
 specifically, “Internet or other electronic network activity information, including, but not limited

¹³ <https://vpnoverview.com/news/google-backpedals-on-claim-that-x-client-data-doesnt-contain-pi-information/>

1 to, browsing history, search history, and information regarding a consumer's interaction with an
2 internet website, application, or advertisement." Cal. Civ. Code § 1798.140(o)(1)(F).

3 89. Google also defines "personal information" to include browsing history in the
4 Chrome Privacy Notice.

5 **D. Chrome's Promise Not To Share PI With Google if Not Synched Was**
6 **Intended To Encourage, Not Diminish, User Engagement**

7 90. Google's motivation to breach its privacy promises to Un-Synched Chrome Users
8 was to increase user engagement and increase revenue for Google. Higher user engagement means
9 more revenue in that moment for Google, and also more data about the users that can lead to more
10 revenue. By promising more privacy, Google induces more private sharing, which is a more
11 profitable kind of user engagement.

12 91. "User engagement" is the degree to which users find products, services and
13 processes interesting or useful. It is typically measured by time spent interacting with products and
14 user satisfaction with that time spent. Engagement can be measured by a variety or combination of
15 activities such as downloads, clicks, interactions, shares, and more.

16 92. Examples of "engagement" data include:

- 17 a. For social or traditional media sites: daily usage, views, time on page, pages
18 per visit, ad clicks, searches, comments, or shares;
- 19 b. For streaming music apps: daily usage, time spent in app, songs listened to,
20 playlists created, friends added;
- 21 c. For an e-commerce store: monthly usage, adding items to cart;
- 22 d. For a personal finance app: weekly usage, sync bank accounts, create a
23 budget, enable notifications, view dashboard; and
- 24 e. Enterprise software: Monthly usage, create reports, share reports, invite
25 users.

26 93. Examples of specific metrics used by online entities to track this engagement include
27 daily active users (DAU), cost-per-acquisition, and ROI. The relative value of these metrics varies
28 by business. For example, high engagement via views or clicks might be good for a news site but

1 not for an insurance app, where more usage might suggest that a user is about to file a claim. Higher
2 engagement leads to higher profits when additional activity leads to purchases, signups,
3 subscriptions, ad views, or clicks.

4 94. Product and marketing teams typically measure user engagement to understand the
5 factors that contribute to higher engagement and use product analytics measure what features affect
6 user behavior. Product analytics and active user engagement data important selling points to
7 advertisers and those who will pay to influences user behavior, whether that is to purchase
8 something, vote or take some other action.

9 95. By inducing more personal and more active engagement, Google can therefore
10 increase its profitability. Because this is a revenue-generating exercise, analytics teams at Google
11 are incentivized to engage in detailed analysis of both how to stimulate more engagement, and also
12 the value of each kind of engagement and the data that it generates. Put differently, specific user
13 engagement are assigned economic value.

14 96. By analyzing user flow—where users spend time, how they interact with others,
15 when they disengage with a site or app or maybe interested in paying more to upgrade—Google
16 can learn valuable insights into how to influence users’ choices and how to target them for Google’s
17 partners. User flow is analyzed by using precisely the metrics at issue in this action.

18 97. Indeed, Google was a pioneer in this field, and Google products help developers
19 create Engagement Scores for users.¹⁴ In June 2011 Google acquired PostRank, specifically
20 because PostRank had an effective tool for measuring user engagement. According to a Google
21 spokesperson at that time, Google is “always looking for new ways to measure and analyze data,”
22 and PostRank would help “make this data more actionable and accountable [through] an innovative
23 approach to measuring web engagement [that can] help us improve our products for our users and
24 advertisers.¹⁵

25
26 _____
27 ¹⁴ <https://www.chromium.org/developers/design-documents/site-engagement>

28 ¹⁵ <https://techcrunch.com/2011/06/03/google-acquires-postrank-an-analytics-service-for-the-social-web/>

1 98. As applied here, the data that Chrome has sent to Google in violation of its promises
2 not to do so is integral to the calculation of users' engagement scores. It can also be tied to specific
3 profitability.

4 99. The most powerful of all of these may be the x-client-referrer header, described
5 above. Because it is all-pervasive and impossible to remove from users' activity, the richness of
6 the data Google collects has higher value than disconnected data points of less robust detail.

7 100. By targeting advertising at users who have a higher amount of "tracked"
8 engagement, Google can increase the profits they make from gathering that data.

9 101. An "untracked" user may only be shown generic ads. Such ads, in turn, tend to yield
10 a lower engagement rate and therefore generate less profit for Google. A "tracked" user's browsing,
11 in contrast, yields greater data for Google to target and is also a more lucrative target in its own
12 right. The more active a user is, the more vulnerable to targeting she is, and more valuable as well.

13 102. In addition, promising a user that she is free from tracking induces a different set of
14 expectations and also a different kind of engagement. Specifically, one would expect a user to
15 engage more actively and more intimately under the belief that she is untracked. She may also
16 engage with different types of content than she would if she knew she were being surveilled,
17 exposing them as relevant for further categories of valuable advertising.

18 103. Tracking users' engagement across Google's advertising products also allows
19 greater optimization of those advertising products, with respect to those individual users, to increase
20 the likelihood of their future engagement with ads, further increasing Google's ability to generate
21 profit.

22 104. By sending to Google Un-Synced Chrome users' data reflecting their behavior,
23 Google is able to draw a more complete picture of those users, even when they had not opted-in to
24 such tracking.

25 105. All of this results in concrete, ascertainable financial gain for Google, directly
26 attributable by the increased user engagement. Those profits can be identified and quantified;
27 indeed, teams of analysts at Google are engaged in precisely this process.
28

1 **E. How Google Instructs Chrome to Report PI to Google**

2 106. Chrome is a web-browser—a software application that enables users to exchange
3 electronic communications over the Internet.

4 107. Every website is hosted by a computer server through which the entity or person in
5 charge of the website exchanges communications with Internet users via users' web-browsers.

6 108. The process through which Chrome transmits communications between users and
7 the first-party websites with which users are communications is called packet-switching.¹⁶

8 109. The prior technology through which phone communications were transmitted was
9 called circuit-switching. With circuit-switching, the service provider would establish a single
10 pathway (or circuit) through which the content of a communication would flow between the parties
11 to the communication. The problem with circuit-switching is that, if the single path becomes
12 blocked, the communication fails.

13 110. Enter packet-switching. With packet-switching, there is no single, dedicated path
14 through which the contents of a communication flow. Instead, the contents of a communication are
15 broken down into dozens, hundreds, or thousands of packets—each of which is routed over a
16 network with different paths to the destination. Each packet contains part of the content and
17 information about its destination. Each packet travels independently to the destination and every
18 packet may travel by a different route to the destination. As the packets arrive, they are arranged
19 by the device to which they are sent. Only at the end are they put both together and the
20 communication formed. The path of each packet, and the order in which each packet arrives, is not
21 relevant to the ultimate success of a communication. Some packets may get stopped in the
22 process—in which case they are resent down a different path.

23 111. Packet-switching is now ubiquitous. For example, all 4G and 5G voice or data
24 communications are made via packet-switching technology.

25 112. Thus, although common imagination may suppose that a modern cellphone call or
26 internet communication involves a direct line of communication between the participants to the

27 _____
28 ¹⁶ Packet-switching is also explained in *U.S. v. Szymuszkiewicz*, 622 F.3d 701, 704 (7th Cir. 2010).

1 communication, that is not true at all. Through packet-switching, the contents of the communication
2 are broken down into dozens, hundreds, or thousands of different packets that are exchanged
3 through separate pathways between the parties to the communication.

4 113. On the Internet, when a user begins a communication with a website, the user's
5 browser starts and continues several processes all at once. These simultaneous processes include:

- 6 a. sending contents of the users' side of the communication to the website;
- 7 b. receiving and rendering the website's side of the communication;
- 8 c. placing the content of the communication in temporary and intermediate
9 storage, and;
- 10 d. in some cases, re-directing the contents of the communication to third-parties;

11 114. The basic commands that Chrome uses to send the users' side of a communication
12 are called GET and POST requests.

13 115. When a user types [https://www.mercurynews.com/2020/05/24/qa-mental-health-](https://www.mercurynews.com/2020/05/24/qa-mental-health-tips-for-handling-the-pandemic/)
14 [tips-for-handling-the-pandemic/](https://www.mercurynews.com/2020/05/24/qa-mental-health-tips-for-handling-the-pandemic/) into her browser (or takes the technological shortcut of clicking a
15 hyperlink), Chrome contacts the website hosting the Mercury News and sends the following
16 communication: "GET 2020/05/24/qa-mental-health-tips-for-handling-the-pandemic/".

17 116. If instead the user were filling out a form on that website and clicks a button to
18 submit the information in the form, Chrome similarly makes connection with the website server
19 but instead sends a "POST" request that includes the specific content that the user placed in the
20 form.

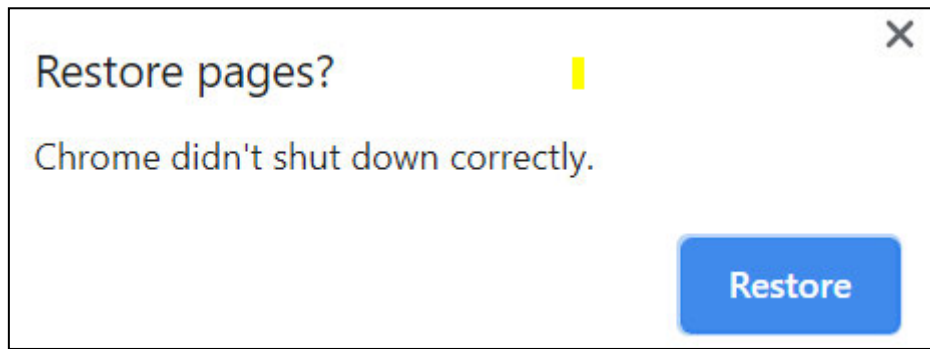
21 117. When a user clicks a hyperlink or hits ENTER to send a communication, Chrome
22 determines whether it is a GET or POST request based on the source code within the browser or
23 the current website with which the user is communicating. The browser then simultaneously:

- 24 a. Places the contents of the GET or POST request in storage in the browser's
25 web-browsing history and short-term memory; and
- 26 b. Connects to and begins a back-and-forth the two-way communication
27 exchange between the user and the website.

28 118. Chrome stores the contents of the communication for at least two purposes:

- 1 a. content is placed in the browser's short-term memory so that, if the user's
- 2 web-browser crashes unexpectedly, when the user re-starts their browser, the
- 3 browser will be able to offer the user the ability to return to their last
- 4 communications prior to the browser's crash; and
- 5 b. The content is placed in the user's browsing history and the user's future
- 6 reference for 90 days.

7 119. For short-term memory, if Chrome crashes unexpectedly and the user re-opens it,
8 Chrome provides the user with the following options at the upper right-hand side of the screen:



- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17 120. This short-term storage is for purposes of back-up protection.
- 18 121. The storage for 90 days in the user's browsing history is temporary, intermediate
- 19 storage incidental to the contemporaneous transmission of the communication.
- 20 122. In response to receiving a GET or POST request from a user, the server for the
- 21 website with which the user is exchanging a communication will send a set of instructions to
- 22 Chrome, commanding Chrome with source code on:
- 23 a. How to render the website's portion of the communication; and
 - 24 b. In some cases (up to 86 percent of popular websites), using source code
 - 25 provided by Google and specifically designed to command the Chrome to
 - 26 contemporaneously re-direct the precise content of the GET or POST part of
 - 27 the communication to Google and its various entities attached to personal
 - 28

1 information and other browser-generated data about the content of the
2 website's portion of the communication.

3 123. Google instructs developers to place its source code that commands Chrome to
4 contemporaneously re-direct the contents of the communication exchanged between the user and
5 the website to Google in the website's header—i.e., before the website's instructions regarding the
6 contents of its side of the communication. For example, for Google Tag Manager, Google instructs
7 developers to place its code “as close to the opening <head> tag as possible on every page of your
8 website[.]”¹⁷

9 124. Google's placement is designed to put priority on the re-directions of content and
10 user personal information from Chrome to Google. By placing the re-direction commands first,
11 Google ensures that the re-direction will occur as soon as possible so that Google will be able to
12 collect the contents and personal information even if the user quickly changes their mind or the
13 browser unexpectedly shuts down before the communication transmissions are complete.

14 125. The transmission process between Chrome and the website server is not discrete,
15 but instead involves a series of rapid, continuing, simultaneous data exchanges between Chrome
16 and the website server with data flowing both ways throughout the process and through dozens,
17 hundreds, or even thousands of different paths to reach their destination at the user or website.¹⁸

18 126. The data and content exchanges between Chrome and the website server continue
19 even after it appears that the website's portion of the communication has been fully rendered on
20 the user's screen.

21 127. At the same time that the transmission and content exchange of the communication
22 is happening between the user's browser and the website server (i.e. the devices), the contents of
23 the communication (including the user's specific request and information about the substance of
24 website's side of the communication) are re-directed to third-parties.

25
26 _____
¹⁷ See <https://developers.google.com/tag-manager/quickstart>

27 ¹⁸ In one example of which counsel is aware, a recording of a single 288 second communication
28 resulted in 22,779 separate packet transmissions—or 79 data packet transmissions per second.

1 128. The Google and Chrome browser-generated redirections of the contents of the
2 communication occur:

- 3 a. Without any further action of the user;
4 b. While connections and the contents of the communication are still being
5 exchanged between the user and the website; and
6 c. Without exception, while the connection between and the communication
7 between the user and the website is still occurring.

8 129. Google is the most frequent third-party recipient of browser-redirectioned
9 communications.

10 130. The Google source code and Chrome browser-generated re-directions of
11 communications content and personal information from Chrome to Google occurs through a
12 combination placement of web-bugs or tracking pixels and iframes.

13 131. A web-bug or tracking pixel is a 1x1 pixel that is placed on the screen. It is tiny and
14 purposefully designed to remain invisible to the user. The web-bug is a tiny, invisible window
15 through which Google surveils Internet users.

16 132. An iframe is a container in which a web-developer can place content, or, in the case
17 of Google's source code and surveillance tools, can place source code for web-bugs or tracking
18 pixels. In many cases, Google's source code and Chrome browser-generated re-directions are
19 funneled first through an iframe designed by Google through a service called Google Tag Manager.
20 The source code for Google Tag Manager instructs Chrome to make certain that the surveillance
21 tool is invisible, literally stating that the Google Tag Manager iframe should hidden. For example,
22 here is the Google Tag Manager source code crafted by Google for The Mercury News:

```
23 <!-- Google Tag Manager (noscript) -->
24 <noscript><iframe src='https://www.googletagmanager.com/ns.html?id=GTM-TLFP4R' height='0' width='0'
25 style='display:none;visibility:hidden'></iframe></noscript>
26 <!-- End Google Tag Manager (noscript) -->
```

26 133. Google writes the source code for web-developers to deploy for its invisible web-
27 bugs and tracking pixels, and for Google Tag Manager, a vessel Google developed to make it even
28 easier for websites to deploy its surveillance tools. Then, having designed the source code to

1 command the contemporaneous re-direction of the contents of communications and user personal
2 information to itself, Google then designed Chrome to send the personal information to Google
3 *regardless of whether the user is logged-in to Google Sync*, in violation of Chrome’s express
4 promises to users.

5 134. Chrome sends the following personal information to Google when a user exchanges
6 communications with any website that includes Google surveillance source code—again,
7 *regardless of whether a user is logged-in to Google Sync or not*:

- 8 a. The user’s unique, persistent cookie identifiers;
- 9 b. The user’s browsing history in the form of the contents of the users’ GET
10 requests and information relating to the substance, purport, or meaning of the
11 website’s portion of the communication with the user;
- 12 c. In many cases, the contents of the users’ POST communications;
- 13 d. The user’s IP address and User-Agent information about their device; and
- 14 e. The user’s x-client-data identifier.

15 135. Each category of personal information that Chrome sends to Google is a separate
16 violation of Chrome’s Terms of Service and an invasion of users’ privacy. And the aggregate
17 impact of these takings effectively puts users *who opted not to Sync* under Google’s surveillance.

18 **F. A Sample Visit to The San Jose Mercury News Website Using Chrome –**
19 **Comparison Between a “Synched” Session and “Un-synched” Session**

20 136. Suppose a Chrome user wished to access an article on mental health during the
21 Covid-19 pandemic and saw the link below to a relevant article on the San Jose Mercury News,
22 and clicked it:



23
24
25
26
27 137. Immediately upon clicking the link, Chrome places the content of the user’s part of
28 the communication in temporary storage, as described above.

1 138. Chrome also immediately communicates a GET request on behalf of the user to The
2 Mercury News at www.mercurynews.com requesting that The Mercury News exchange its part of
3 the communication by sending a specific article: “Q&A: Mental health tips for handling the
4 pandemic.”

5 139. The specific GET request sent from Chrome to The Mercury News is:

```
6 :authority: www.mercurynews.com  
7 :method: GET  
8 :path: /2020/05/24/qa-mental-health-tips-for-handling-the-pandemic/  
9
```

10 140. The user’s simple act of clicking a mouse to begin the communication with The
11 Mercury News about Mental Health Tips for Handling the Pandemic triggers a set of
12 contemporaneous, ongoing connections between Chrome and The Mercury News—and the
13 contemporaneous redirection of the contents of the communication between the user and The
14 Mercury News to various Google properties.

15 141. Google’s source code and the Chrome browser then immediately re-direct the
16 content of the user’s side of the communication and The Mercury News response to Google Tag
17 Manager, Google Ads, Google DoubleClick, Google Analytics, and Google Captcha.

18 142. Each re-direction of data from Chrome to Google includes one or more of the
19 following: content of the communication, IP address, user-agent information, x-client-data
20 identifier, and various unique, persistent cookies identified herein.

21 143. On July 21, 2020, counsel for the Plaintiffs employed an expert to record data
22 transmissions from the Chrome browser to Google in each of three different browser-states for the
23 example GET request to The Mercury News for the mental health article discussed above. The
24 browser-states tested were: (1) Sync mode where the Google test account had logged-in to Google
25 Sync; (2) Basic-browser mode where the Google test account had not logged-in to Google Sync
26 but was logged into a Google account (here, Gmail); and (3) Basic-browser mode where the Google
27 test account was not logged-in to Google Sync and also not logged into any other Google account.
28

144. The following charts compare the PI that Chrome sends to Google when the browser is one of three states: first, when the user has affirmatively synched with another Google Account (called “synched” below); second, when the user is not synched, but logged into another Google service such as Gmail (“un-synched, with Gmail log-in”); and third, when the user is neither synched nor logged into any other Google account (“un-synched, logged out”). As the test results below confirm, *Google causes Chrome to send PI to itself even when a Chrome user has not authorized the data collection by synching.*

145. Chrome copies and re-directs the content of the user’s GET request (the one asking for the article on mental health) to Google Ads, Google DoubleClick, and Google Analytics in identical fashion *regardless of whether the user is synched.*

PERSONAL INFORMATION CHROME SENDS TO ALL GOOGLE CONTENT OF COMMUNICATION WITH THE MERCURY NEWS Identical for All Browser-States and All Google Entity Recipients	
Synched	2020/05/24/qa-mental-health-tips-for-handling-the-pandemic
Un-Synched, Gmail Login	2020/05/24/qa-mental-health-tips-for-handling-the-pandemic
Un-Synched, no Gmail Login	2020/05/24/qa-mental-health-tips-for-handling-the-pandemic.html

146. Similarly, the x-client-data header Chrome sends to Google Ads, Google DoubleClick, and Google Analytics is identical *regardless of whether the user is synched:*

PERSONAL INFORMATION CHROME SENDS TO GOOGLE X-CLIENT-DATA-HEADER Identical for All Browser-States and All Google Entity Recipients Except Analytics	
Synched	CKy1yQEIkbbJAQimtskBCMS2yQEIQZ3KAQjnyMoBCLTLygE=
Un-Synched, Gmail Login	CKy1yQEIkbbJAQimtskBCMS2yQEIQZ3KAQjnyMoBCLTLygE=
Un-Synched, no Gmail Login	CKy1yQEIkbbJAQimtskBCMS2yQEIQZ3KAQjnyMoBCLTLygE=

147. Similarly, the IP address and User-Agent data Chrome sends to Google Ads, Google DoubleClick, and Google Analytics is identical *regardless of whether the user is synched.*

148. Similarly, the Google Analytics “cid” cookie or “Client ID” that Chrome sends to Google is identical *regardless of whether the user is synched:*

PERSONAL INFORMATION CHROME SENDS TO ALL GOOGLE “CID” – “CLIENT ID” COOKIE VALUE Identical for All Browser-States and All Google Entity Recipients	
Synched	cid=2007029474.1595353114
Un-Synched, Gmail Login	cid=2007029474.1595353114
Un-Synched, no Gmail Login	cid=2007029474.1595353114

1 149. The third-party cookie data Chrome sends to Google Ads is identical for at least 11
 2 different persistent, unique cookies for Un-Synched Chrome users regardless of whether signed
 3 into Gmail, but not transmitted to Google if the Un-Synched Chrome user is not also logged into
 4 Gmail:

PERSONAL INFORMATION CHROME SENDS TO GOOGLE ADS UNIQUE, PERSISTENT THIRD-PARTY COOKIE VALUES Identical for Synched and Un-Synched w/ Gmail Login	
5 Synched	6 SID=zQfoZ_zUnJr9Gm_IL2u7ticWDqZNymdEgeQPEJdMF0tShKy 7 XCg_BgOS7PQHBWgLiW71F4Q. 8 __Secure-3PSID=zQfoZ_zUnJr9Gm_IL2u7ticWDqZNymdEge 9 QPEJdMF0tShKyXryW3ljJQRAkrQ 10 0hbzqbBHg. 11 HSID=AFuEZ4mCJy32UrJK7 12 SSID=Aw06H6mNsRcQYQjqA 13 APISID=U1WjkuS385Vfizcg/AXMK-fI2Ee2PZnjSB 14 SAPISID=tVrmANaeR-_R3mDV/ABTnEns79q7apJgjE 15 __Secure-HSID=AFuEZ4mCJy32UrJK7 16 __Secure-SSID=Aw06H6mNsRcQYQjqA 17 __Secure-APISID=U1WjkuS385Vfizcg/AXMK-fI2Ee2PZnjSB 18 __Secure-3PAPISID=tVrmANaeR-_R3mDV/ABTnEns79q7ap 19 JgjENID=204=Yc40KkubQ69v_6cmRVkl6eEK6FPzgNcuct 20 N7ndjgcsBeMwUO4uxFOCBmFTLG0HNLk7p13a0Le2tnE 21 gjOllwZi62Jh4f4fjKFXMR8pL0Z4GqbjlUtejOv3Nvhtf1D 22 n63dABgRTnJIRXPklAsY5hCMQfLCHCAKIrg01U 23 p3q7q2fFN3Aj8lXaT9g12rT5QtcNgJAZP8dKmLevACA
24 Un-Synched, Gmail Login	25 SID=zQfoZ_zUnJr9Gm_IL2u7ticWDqZNymdEgeQPEJdMF0tShKy 26 XCg_BgOS7PQHBWgLiW71F4Q. 27 __Secure-3PSID=zQfoZ_zUnJr9Gm_IL2u7ticWDqZNymdEge 28 QPEJdMF0tShKyXryW3ljJQRAkrQ 0hbzqbBHg. HSID=AFuEZ4mCJy32UrJK7 SSID=Aw06H6mNsRcQYQjqA APISID=U1WjkuS385Vfizcg/AXMK-fI2Ee2PZnjSB SAPISID=tVrmANaeR-_R3mDV/ABTnEns79q7apJgjE __Secure-HSID=AFuEZ4mCJy32UrJK7 __Secure-SSID=Aw06H6mNsRcQYQjqA __Secure-APISID=U1WjkuS385Vfizcg/AXMK-fI2Ee2PZnjSB __Secure-3PAPISID=tVrmANaeR-_R3mDV/ABTnEns79q7ap JgjENID=204=Yc40KkubQ69v_6cmRVkl6eEK6FPzgNcuct N7ndjgcsBeMwUO4uxFOCBmFTLG0HNLk7p13a0Le2tnE gjOllwZi62Jh4f4fjKFXMR8pL0Z4GqbjlUtejOv3Nvhtf1D n63dABgRTnJIRXPklAsY5hCMQfLCHCAKIrg01U p3q7q2fFN3Aj8lXaT9g12rT5QtcNgJAZP8dKmLevACA
Un-Synched, no Gmail Login	none

1 150. Despite Google's demonstrated ability above to block the transmission of some
 2 cookies, it still causes others to be transmitted, as noted below, *regardless of whether the user is*
 3 *synced*:

PERSONAL INFORMATION CHROME SENDS TO GOOGLE DOUBLECLICK THIRD-PARTY COOKIES – IDE identical for all browser states	
Synched	IDE=AHWqTUluD72jj7k5Rr5ipWileEiyaUdEyFm-N1x6ZCPzZOfbTN0bUarkMjwuYJMV
Un-Synched, Gmail Login	IDE=AHWqTUluD72jj7k5Rr5ipWileEiyaUdEyFm-N1x6ZCPzZOfbTN0bUarkMjwuYJMV
Un-Synched, no Gmail Login	IDE=AHWqTUluD72jj7k5Rr5ipWileEiyaUdEyFm-N1x6ZCPzZOfbTN0bUarkMjwuYJMV

9 151. Finally, Chrome sends other third-party cookie personal identifiers that qualify as
 10 personal information, *regardless of whether the user is synced*. These other cookies have values
 11 that change based on log-in status, but which are associated with the cookie values that are identical
 12 across all browser-states, making them reasonably capable of being associated with specific users:

PERSONAL INFORMATION CHROME SENDS TO GOOGLE DOUBLECLICK COOKIE SYNCHING Identical for All Browser-States	
Synched	ID=8067c38bf1d71e0f:T=1595353118:S=ALNI_MacZyW8MLDn-omh5WOAbbl6y_qlGA
Un-Synched, Gmail Login	ID=8067c38bf1d71e0f:T=1595353118:S=ALNI_MacZyW8MLDn-omh5WOAbbl6y_qlGA
Un-Synched, no Gmail Login	ID=8067c38bf1d71e0f:T=1595353118:S=ALNI_MacZyW8MLDn-omh5WOAbbl6y_qlGA

18 152. Combined, the data that Google causes Chrome to send to itself (illustrated above)
 19 demonstrates that Google has designed Chrome to collect massive amounts of user personal
 20 information and linked to websites visited, regardless whether the Chrome user synced.

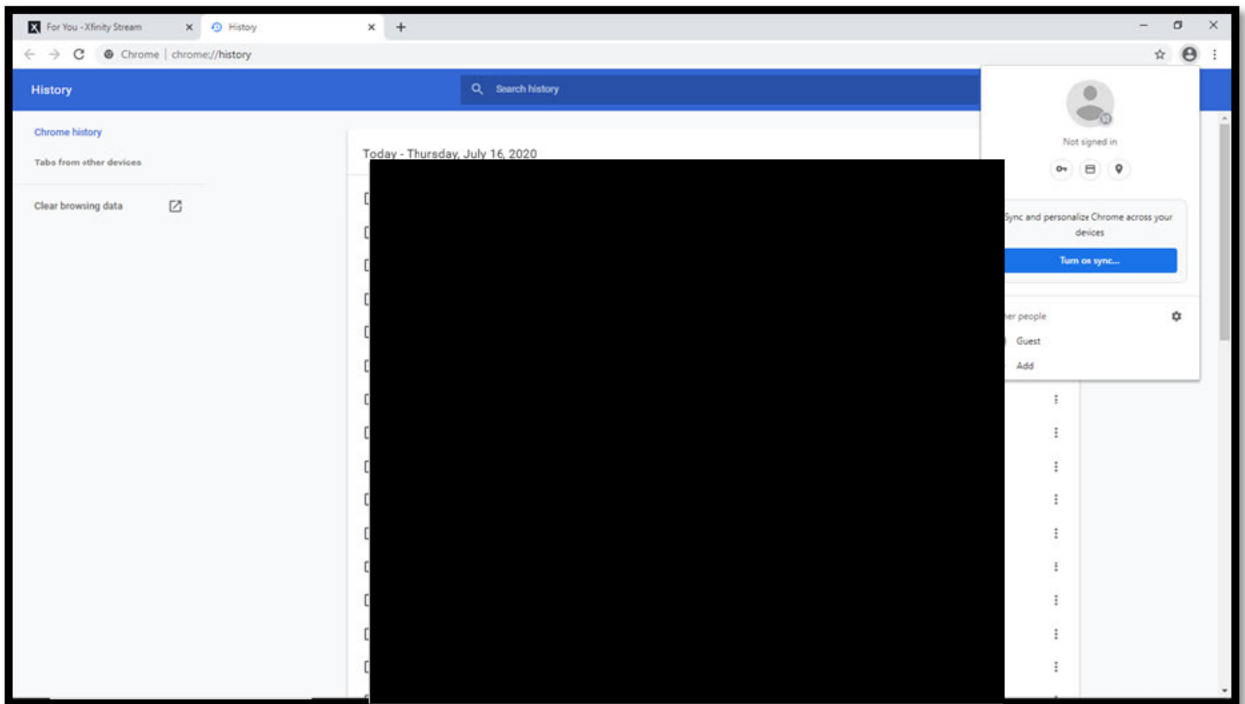
21 153. Even worse, most of the PI is collected in forms other than cookies (for example, IP
 22 address + user-agent data and the x-client-data identifier) meaning that Chrome will still transmit
 23 the data even if the user is using cookie blockers.

G. Plaintiffs' Personal Experiences

Plaintiff Patrick Calhoun

154. On Saturday, July 18, 2020, Plaintiff Patrick Calhoun used Fiddler to recreate and record data transmission that Chrome sent from his personal computing device to Google related to websites he had visited earlier in the Relevant Period.

155. Plaintiff Calhoun recorded that, per his usual practice, he was not logged-in to Google Sync at the time of the recording:



156. Plaintiff Calhoun then recorded data transmissions that Chrome sent to Google when he exchanged communications with [REDACTED] government and political articles from earlier in the week.

157. For the government communication, Chrome sent the following personal information to Google even though Calhoun was not logged-in to Sync:

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

```

Request Headers
GET [Redacted]
Client
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
User-Agent: [Redacted]
Miscellaneous
Referer: https://www.[Redacted]
Security
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Transport
Connection: keep-alive
Host: www.google-analytics.com

```

158. The data Chrome sent to Google Analytics included his IP address, User-Agent information, and CID identifier as well as the content of the communication:

```

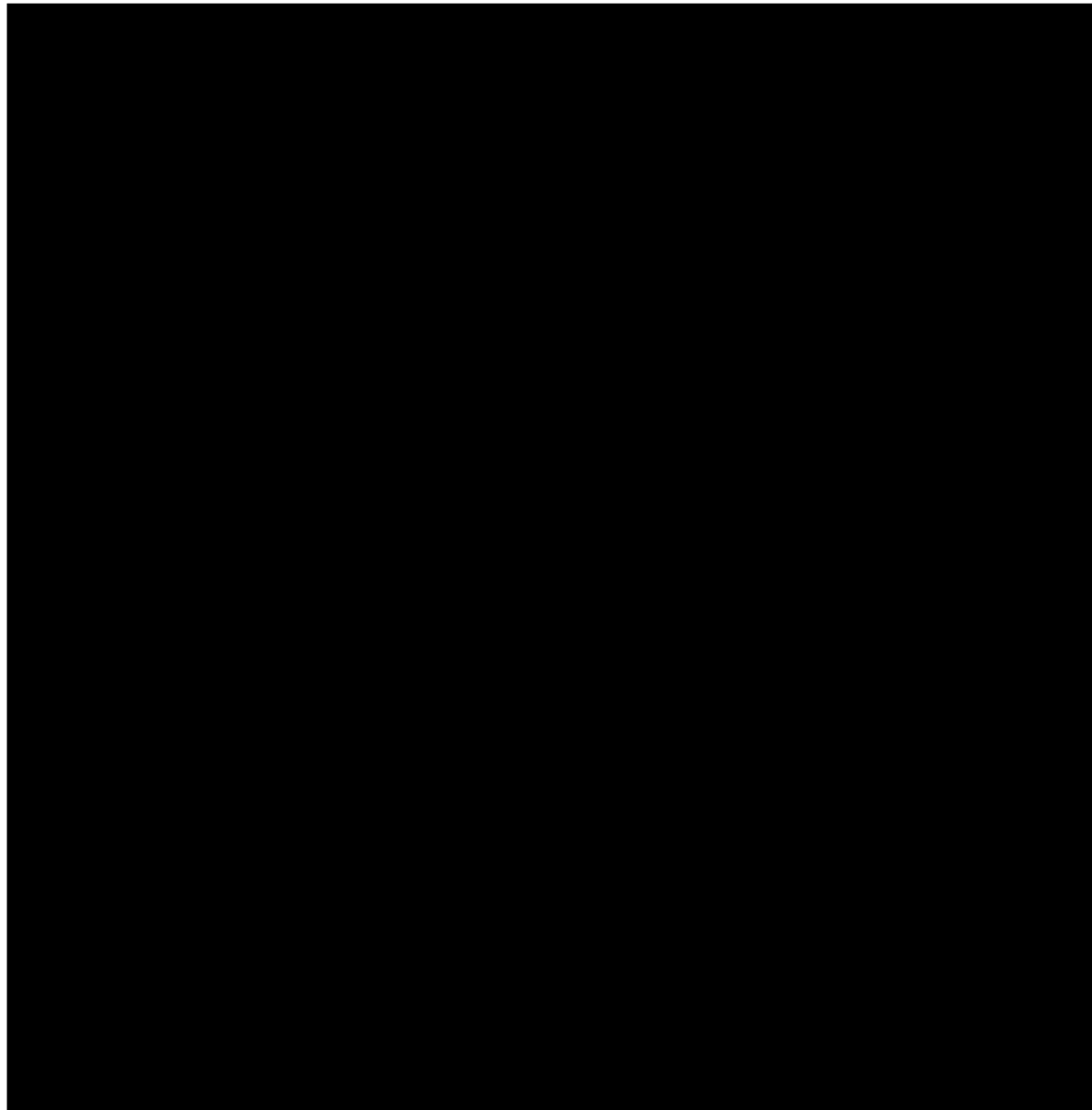
Request Headers
GET [Redacted]
Client
Accept: /*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
User-Agent: [Redacted]
Cookies
Cookie
1P_JAR=2020-07-17-21 [Redacted]
ANID=[Redacted]
NID=[Redacted]
Miscellaneous
Referer: https://www.[Redacted]
X-Client-Data: [Redacted]
X-Omnibox-OpenDevice-Suggestions: Control_V2
Security
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Transport
Connection: keep-alive
Host: www.google.com

```

159. The data Chrome sent to Google.com included his IP address, User-Agent information, X-Client-Data identifier, unique cookie identifiers as well as the content of the communication—a request to load the webpage for the [Redacted]

[Redacted]
[Redacted]
[Redacted]
[Redacted] all of which Google is aware through its web-crawlers:

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



160. In addition to Calhoun's personal information about his [REDACTED] communication with the [REDACTED], Chrome also sent to Google the exact date and time of Calhoun's communication. Over time, Chrome would disclose the exact date and time of every time Calhoun went to this website.

161. For the article of political interest, Chrome sent the following information to Google.com even though Calhoun was not logged-in to Sync:

```

1  Headers  TextView  SyntaxView  WebForms  HexView  Auth  Cookies  Raw  JSON  XML
2  GET [REDACTED]
3  Client
4  Accept: */*
5  Accept-Encoding: gzip, deflate, br
6  Accept-Language: en-US,en;q=0.9
7  User-Agent: [REDACTED]
8  Cookies
9  Cookie
10  IP_1AP=2020-07-17-21
11  ANID=[REDACTED]
12  NID=[REDACTED]
13  204=[REDACTED]
14  Miscellaneous
15  Referer: https://www.[REDACTED]
16  X-Client-Data: [REDACTED]
17  X-Omnibox-On-Service-Suggestions: Control_V2
18  Security
19  Sec-Fetch-Dest: script
20  Sec-Fetch-Mode: no-cors
21  Sec-Fetch-Site: cross-site
22  Transport
23  Connection: keep-alive
24  Host: adservice.google.com

```

162. The X-Client-Data identifier, IP address, User-Agent, and NID cookie sent to Google for this communication is identical to the PI Chrome sent to Google following Calhoun's visit to the prior website (allowing his web browsing history to be comprehensively monitored), except here, the content of the communication in the URL is different.

163. Chrome also improperly sent the following PI to Google DoubleClick:

```

14  Request Headers  [How?] [Header Information]
15  POST [REDACTED]
16  Client
17  Accept: */*
18  Accept-Encoding: gzip, deflate, br
19  Accept-Language: en-US,en;q=0.9
20  User-Agent: [REDACTED]
21  Cookies
22  Cookie
23  DSID=NO_DATA
24  IDE=[REDACTED]
25  Entity
26  Content-Length: 0
27  Content-Type: text/plain;charset=UTF-8
28  Miscellaneous
29  Referer: [REDACTED]
30  X-Client-Data: [REDACTED]
31  Security
32  Origin: https://www.aol.com
33  Sec-Fetch-Dest: empty
34  Sec-Fetch-Mode: no-cors
35  Sec-Fetch-Site: cross-site
36  Transport
37  Connection: keep-alive
38  Host: googleads4.g.doubleclick.net

```

164. Once again, the X-Client-Data identifier, IP address, and User-Agent sent to Google DoubleClick for this communication is identical to the personal information Chrome sent to Google at the prior website, allowing for association of multiple websites with the same person.

165. In addition, the IDE cookie identifier is identical to the IDE cookie identifier that Chrome would share with Google DoubleClick for communication with a communication exchanged with a website that has deployed Google's DoubleClick source code.

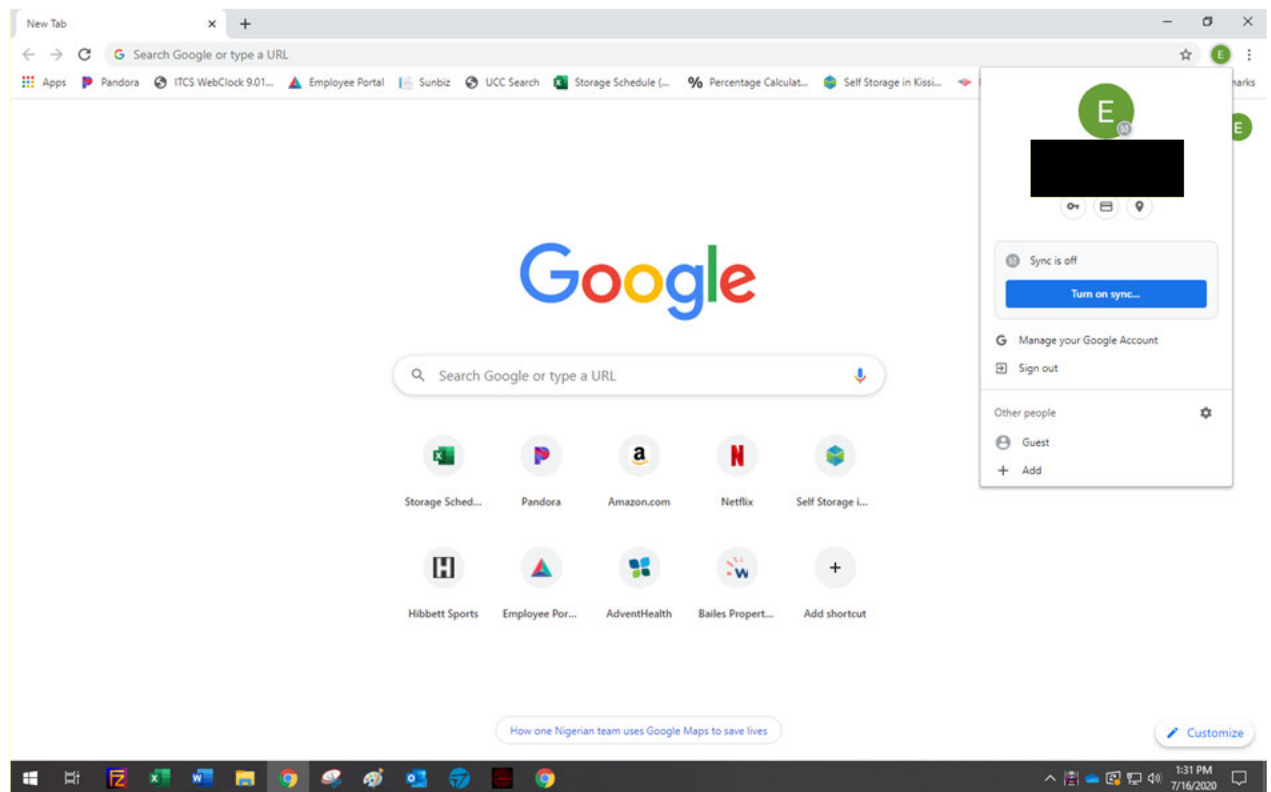
166. Further, Chrome disclosed an "adsid" cookie syncing value that would be identical if Calhoun had actually been logged-in to Google Sync.

1 167. Despite its promises to the contrary, Google combined Plaintiff Calhoun’s personal
2 information that it obtained when he was not logged-in to Google Sync with other data it has about
3 him, and will use that data to place Calhoun in advertising categories from which Google will profit
4 from targeted advertising to him based on data that it did not have the right to obtain—including
5 but not limited to recordings captured and detailed herein, that Calhoun communicates with the
6 [REDACTED] and that he
7 reads political articles with [REDACTED]

8 *Plaintiff Elaine Crespo*

9 168. On Friday, July 17, 2020, Plaintiff Elaine Crespo used Fiddler to recreate and record
10 data transmissions that Chrome sent from her personal computing device to Google related to
11 websites she had visited earlier in the Relevant Period.

12 169. Plaintiff Crespo recorded that, per her usual practice, she was not logged-in to
13 Google Sync at the time of the recording:



1 170. Plaintiff Crespo then recorded data transmissions that Chrome sent to Google when
 2 she exchanged Internet communications with her bank. She recorded that Chrome sent the
 3 following personal information to Google even though Crespo was not logged-in to Sync:

4

```

Request Headers [Raw] [Header Definitions]
5 GET [REDACTED]
Cache
6 cache-control: no-cache
  pragma: no-cache
Client
7 accept: image/webp,image/apng,image/*,*/*;q=0.8
  accept-encoding: gzip, deflate, br
  accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
  user-agent: [REDACTED]
Cookies
9 [x] cookie
  [REDACTED]
  [REDACTED]
  [REDACTED]
  [REDACTED]
  [REDACTED]
  ANID=[REDACTED]
  CONSENT=YES+US.en+202005
  [x] NID
  204=[REDACTED]
Miscellaneous
13 referer: [REDACTED]
  x-client-data: [REDACTED]
Security
14 sec-fetch-dest: image
  sec-fetch-mode: no-cors
  sec-fetch-site: cross-site
Transport
16 Host: www.google.com
  
```

17

18 171. Google also caused Chrome to send the following to Google:

19

20

21

22

23

24

25

26

27

28

1 Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML [Raw] [Header Definitions]

2 Request Headers

3 GET

4 Cache

- cache-control: no-cache
- pragma: no-cache

5 Client

- accept: image/webp,image/apng,image/*,*/*;q=0.8
- accept-encoding: gzip, deflate, br
- accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
- user-agent: [REDACTED]

6 Cookies

- cookie
- IDE=[REDACTED]

7 Miscellaneous

- referer: https://[REDACTED]
- x-client-data: [REDACTED]

8 Security

- sec-fetch-dest: image
- sec-fetch-mode: no-cors
- sec-fetch-site: cross-site

9 Transport

- Host: ad.doubleclick.net

11 Request Headers [Raw] [Header Definitions]

12 GET

13 Cache

- cache-control: no-cache
- pragma: no-cache

14 Client

- accept: image/webp,image/apng,image/*,*/*;q=0.8
- accept-encoding: gzip, deflate, br
- accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
- user-agent: [REDACTED]

15 Cookies

- cookie
- IDE=[REDACTED]

16 Miscellaneous

- referer: https://[REDACTED]
- x-client-data: [REDACTED]

17 Security

- sec-fetch-dest: image
- sec-fetch-mode: no-cors
- sec-fetch-site: cross-site

18 Transport

- Host: googleads.g.doubleclick.net

19 < >

20

21

22 172. When Crespo logged-out of her bank account, Google knew, at the exact moment it

23 happened, because Chrome improperly shared this fact and other PI with Google Ads and Google

24 DoubleClick.

25

26

27

28

Request Headers [Raw] [Header Definitions]

1 GET

2

3 **Cache**
cache-control: no-cache
pragma: no-cache

4 **Client**
accept: image/webp,image/apng,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
user-agent: [REDACTED]

5 **Cookies**
[REDACTED]

6 cookie
__Secure-3PAPISID=[REDACTED]
__Secure-3PSID=[REDACTED]
__Secure-APISID=[REDACTED]
__Secure-HSID=[REDACTED]
__Secure-SSID=[REDACTED]
ANID=[REDACTED]
CONSENT=YES+US.en+202005

7

8 NID
204=[REDACTED]

9 **Miscellaneous**
referrer: [REDACTED]
x-client-data: [REDACTED]

10 **Security**
sec-fetch-dest: image
sec-fetch-mode: no-cors
sec-fetch-site: cross-site

11 **Transport**
Host: adservice.google.com

12

13

Request Headers [Raw] [Header Definitions]

14 GET

15

16 **Cache**
cache-control: no-cache
pragma: no-cache

17 **Client**
accept: image/webp,image/apng,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9,es-US;q=0.8,es;q=0.7
user-agent: [REDACTED]

18 **Cookies**
[REDACTED]

19 cookie
IDE=[REDACTED]

20 **Miscellaneous**
referrer: [REDACTED]
x-client-data: [REDACTED]

21 **Security**
sec-fetch-dest: image
sec-fetch-mode: no-cors
sec-fetch-site: cross-site

22 **Transport**
Host: googleads.g.doubleclick.net

23

24

25 173. Despite its promises to the contrary, Google combined Plaintiff Crespo's PI that it

26 obtained when she was not logged-in to Google Sync with other data it has about her, and will use

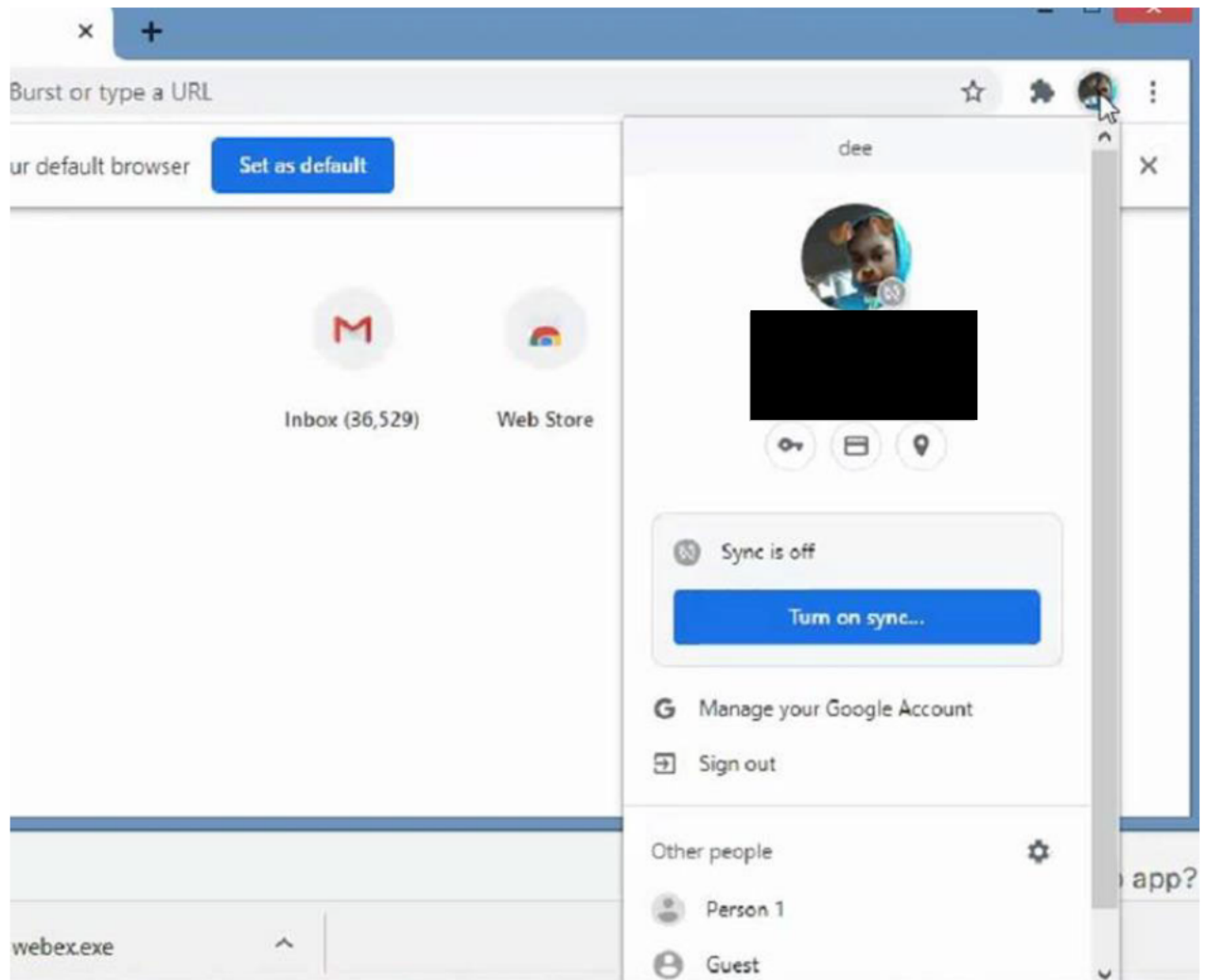
27 that data to place her in advertising categories from which Google will profit from targeted

28 advertising to her based on data that it did not have the right to obtain.

Plaintiff Hadiyah Jackson

174. On Thursday, July 16, 2020, Plaintiff Hadiyah Jackson used Fiddler to recreate and record data transmissions that Chrome sent from her personal computing device to Google related to websites she had visited earlier in the Relevant Period.

175. Plaintiff Jackson recorded that, per her usual practice, she was not logged-in to Google Sync at the time of the recording:



176. Plaintiff Jackson then recorded data transmissions that Chrome sent to Google with the exchange of communications with [REDACTED] government.

177. For the government communications, Chrome sent the following personal information to Google even though Jackson was not logged-in to Sync:

Request Headers [Raw] [Header Definitions]

1 GET [REDACTED]

2 **Cache**
cache-control: no-cache
pragma: no-cache

3 **Client**
accept: image/webp,image/apng,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
4 user-agent: [REDACTED]

5 **Cookies**
[REDACTED] cookie
[REDACTED] Secure-3PAPISID [REDACTED]
[REDACTED] Secure-3PSID= [REDACTED]
[REDACTED] Secure-APISID [REDACTED]
[REDACTED] Secure-HSID= [REDACTED]
[REDACTED] Secure-SSID= [REDACTED]
[REDACTED] 1P_JAR=2020-07-16-17
[REDACTED] ANID= [REDACTED]
[REDACTED] APISID= [REDACTED]
[REDACTED] HSID= [REDACTED]
[REDACTED] NID [REDACTED]
[REDACTED] 204 [REDACTED]
[REDACTED] SAPISID [REDACTED]
[REDACTED] SID= [REDACTED]
[REDACTED] SIDC [REDACTED]
[REDACTED] SSID [REDACTED]

6 **Miscellaneous**
7 referer: [REDACTED]

8 **Transport**
9 Host: www.google.com

10 < [REDACTED] >

11

12

13

14 178. Chrome also improperly sent the following PI to Google Analytics:

15

16

17

18

19

20

21

22

23

24

25

26

27

28

QueryString	
Name	Value
v	1
_v	j83
a	[REDACTED]
t	pageview
_s	1
dl	[REDACTED]
ul	en-us
de	UTF-8
dt	[REDACTED]
sd	24-bit
sr	1366x768
vp	811x632
je	0
_u	[REDACTED]
jid	[REDACTED]
gid	[REDACTED]
cid	[REDACTED]
tid	[REDACTED]
_gid	[REDACTED]
_r	1
gtm	[REDACTED]
z	[REDACTED]

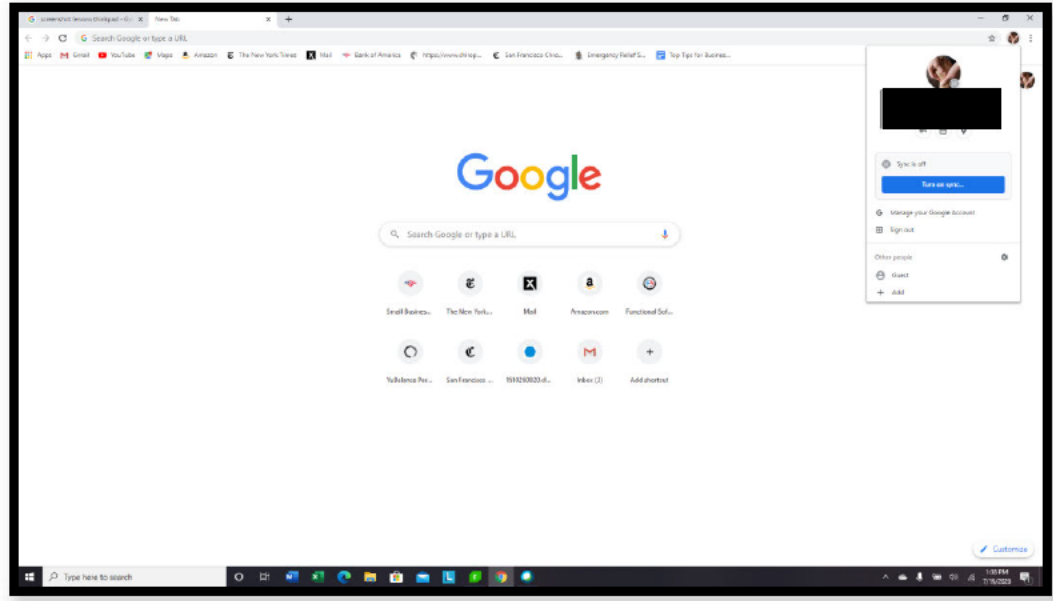
179. Despite its promises to the contrary, Google combined Plaintiff Jackson's personal information that it obtained when she was not logged-in to Google Sync, including communications relating to [REDACTED] with other data it has about her, and will use that data to place Jackson in advertising categories from which Google will profit from targeted advertising to her based on data that it did not have the right to obtain.

Plaintiff Claudia Kindler

180. On Sunday, July 19, 2020, Plaintiff Claudia Kindler used special software called Fiddler to recreate and record data transmissions that Chrome sent from her personal computing device to Google while visiting websites that she had visited earlier in the Relevant Period.

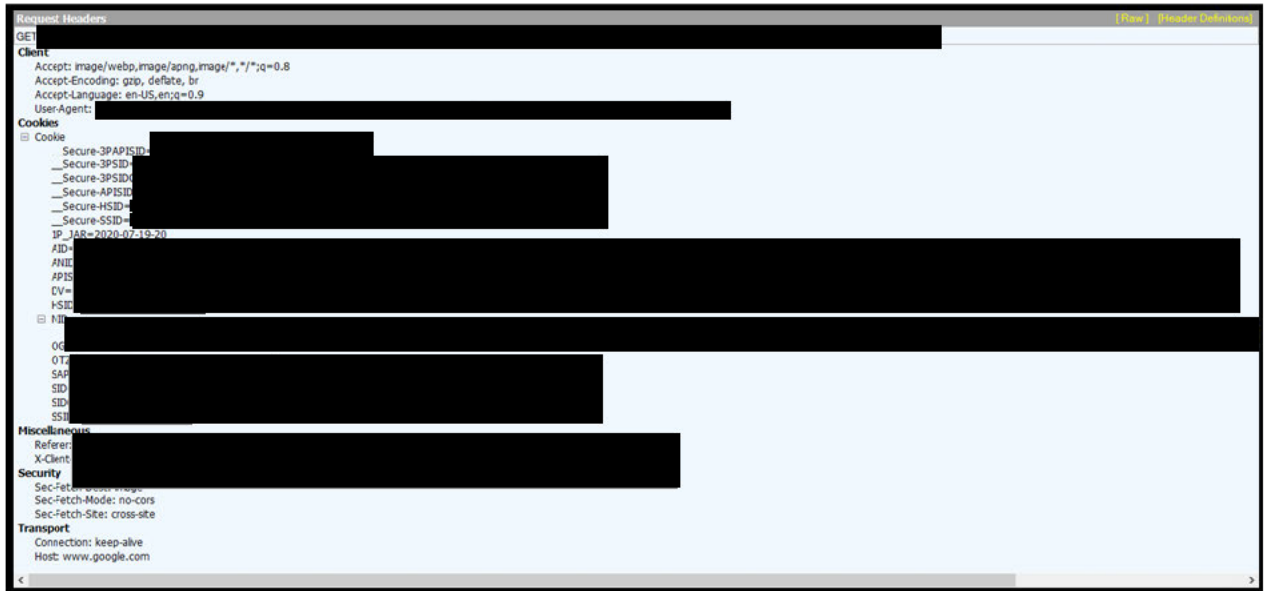
181. Plaintiff Kindler recorded that, per her usual practice, she was not logged-in to Google Sync at the time of the recording:

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



182. Plaintiff Kindler then recorded data transmissions that Chrome sent to Google when she exchanged communications with her healthcare provider, her bank, and her continuing professional education provider.

183. For her healthcare provider, Chrome sent the following PI to Google despite the fact that Kindler was not logged-in to Sync:



184. Although she was not logged-in to Sync, Chrome disclosed Kindler's personal information to Google that included the fact that Kindler was communicating with her healthcare

1 provider, the X-Client-Data-identifier, IP address, User-Agent, the cookie-synching “cid” value,
2 and 11 different Google.com cookies that are also associated with her Google account.

3 185. At the time of the communication, the website would have appeared like this—with
4 the option to reserve a spot at an [REDACTED]



14 186. When Kindler took action to “Save [Her] Spot at [REDACTED]” Chrome sent the
15 following PI to Google Analytics:
16
17
18
19
20
21
22
23
24
25
26
27
28

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

QueryString	
Name	Value
v	1
__v	[REDACTED]
alp	1
a	[REDACTED]
t	event
__s	1
dl	[REDACTED]
ul	en-us
de	UTF-8
dt	[REDACTED]
sd	24-bit
sr	1920x1080
vp	1920x969
je	0
ec	Conversion Action
ea	[REDACTED]
el	[REDACTED]
__u	[REDACTED]
jid	[REDACTED]
gjid	[REDACTED]
cid	[REDACTED]
tid	[REDACTED]
__gid	[REDACTED]
__r	1
cd43	[REDACTED]
cd47	[REDACTED]
cm46	[REDACTED]
z	[REDACTED]

187. Chrome also contemporaneously sent the following PI to Google DoubleClick:

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML | [Raw] [Header D]

Request Headers

GET [REDACTED]

Client

Accept: image/webp,image/apng,image/*,*/*;q=0.8
 Accept-Encoding: gzip, deflate, br
 Accept-Language: en-US,en;q=0.9
 User-Agent: [REDACTED]

Cookies

Cookie
 IDE=[REDACTED]

Miscellaneous

Referer: https://www.[REDACTED]

Security

Sec-Fetch-Dest: image
 Sec-Fetch-Mode: no-cors
 Sec-Fetch-Site: cross-site

Transport

Connection: keep-alive
 Host: stats.g.doubleclick.net

188. When she visited her bank's website, Chrome improperly sent the following personal information to Google even though Kindler was not logged-in to Sync:

Request Headers [Raw] [Header Definitions]

GET [REDACTED]

Client
 Accept: image/webp,image/apng,image/*,*/*;q=0.8
 Accept-Encoding: gzip, deflate, br
 Accept-Language: en-US,en;q=0.9
 User-Agent: [REDACTED]

Cookies
 Cookie [REDACTED]
 __Secure-3PAPI [REDACTED]
 __Secure-3PSID [REDACTED]
 __Secure-3PSID [REDACTED]
 __Secure-APISID [REDACTED]
 __Secure-HSID [REDACTED]
 __Secure-SSID [REDACTED]
 IP_JAR=2020-07-19-21
 ANID [REDACTED]
 APIS [REDACTED]
 DV=[REDACTED]
 HSID [REDACTED]
 NID [REDACTED]
 OGPC [REDACTED]
 OTZ=[REDACTED]
 SAPIS [REDACTED]
 SID=[REDACTED]
 SIDCC [REDACTED]
 SSID=[REDACTED]

Miscellaneous
 Referer: https://www [REDACTED]
 X-Client-Data: [REDACTED]

Security
 Sec-Fetch-Dest: image
 Sec-Fetch-Mode: no-cors
 Sec-Fetch-Site: cross-site

Transport
 Connection: keep-alive
 Host: www.google.com

189. When Kindler logged-out of her banking account, Chrome even informed Google of this fact:

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

Request Headers [Raw] [Header Definitions]

GET [REDACTED]

Client
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 Accept-Encoding: gzip, deflate, br
 Accept-Language: en-US,en;q=0.9
 User-Agent: [REDACTED]

Cookies
 Cookie [REDACTED]
 IDE=[REDACTED]

Miscellaneous
 Referer: http [REDACTED]
 X-Client-Data: [REDACTED]

Security
 Sec-Fetch-D [REDACTED]
 Sec-Fetch-Mode: navigate
 Sec-Fetch-Site: cross-site
 Upgrade-Insecure-Requests: 1

Transport
 Connection: keep-alive
 Host: 1359940.fs.doubleclick.net

1 190. When she visited the website of her continuing education provider, once again
 2 Google was her uninvited guest, monitoring every step and improperly collecting the following PI
 3 despite the fact that Kindler was not Synched with any Google account:

4

5 **Request Headers** [Raw] [Header Definitions]

6 **GET** [REDACTED]

7 **Client**
 Accept: image/webp,image/apng,image/*,*/*;q=0.8
 Accept-Encoding: gzip, deflate, br
 Accept-Language: en-US,en;q=0.9
 User-Agent: [REDACTED]

8 **Cookies**
 [REDACTED]

9 **Cookie**
 [REDACTED]

10 1P_JAR=2020-07-19-21
 ANID=[REDACTED]
 APIS=[REDACTED]
 DV=[REDACTED]
 HSID=[REDACTED]
 NID=[REDACTED]
 OGP=[REDACTED]
 OTZ=[REDACTED]
 SAPIS=[REDACTED]
 SID=[REDACTED]
 SIDC=[REDACTED]
 SSID=[REDACTED]

11 **Miscellaneous**
 Referer: [REDACTED]
 X-Client: [REDACTED]

12 **Security**
 Sec-Fetch-Dest: image
 Sec-Fetch-Mode: no-cors
 Sec-Fetch-Site: cross-site

13 **Transport**
 Connection: keep-alive
 Host: www.google.com

14

15

16

17

18

19

20

21 191. Chrome also sent Kindler's personal information to Google DoubleClick:

22

23

24

25

26

27

28

1 Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML | [Raw] [Header Definitions]

2 Request Headers

3 GET [REDACTED]

4 Client

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

6 Accept-Encoding: gzip, deflate, br

7 Accept-Language: en-US,en;q=0.9

8 User-Agent [REDACTED]

9 Cookies

10 [REDACTED]

11 Miscella

12 Referer [REDACTED]

13 X-Client [REDACTED]

14 Security

15 Sec-Fetch-Dest: iframe

16 Sec-Fetch-Mode: navigate

17 Sec-Fetch-Site: cross-site

18 Upgrade-Insecure-Requests: 1

19 Transport

20 Connection: keep-alive

21 Host: bid.g.doubleclick.net

192. And Chrome sent Kindler’s personal information to Google Analytics:

11 Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

12 QueryString

Name	Value
v	1
__v	[REDACTED]
a	[REDACTED]
t	pageview
__s	1
dl	https:// [REDACTED]
ul	en-us
de	UTF-8
dt	[REDACTED]
sd	24-bit
sr	1920x1080
vp	1903x969
je	0
__u	[REDACTED]
jid	[REDACTED]
gjid	[REDACTED]
cid	[REDACTED]
tid	[REDACTED]
__gid	[REDACTED]
gtm	[REDACTED]
z	[REDACTED]

193. Despite its promises to the contrary, Google combined Plaintiff Kindler’s personal information that it obtained when she was not logged-in to Google Sync, including that she was a patient who scheduled an appointment at [REDACTED] has an account at [REDACTED] and is taking continuing education courses on [REDACTED] Google combines this with other data is has

1 about her and will use that data to place Kindler in advertising categories from which Google will
2 profit from targeted advertising to her based on data that it did not have the right to obtain.

3 **H. Google’s Improper Collection of PI from Plaintiffs and Other Un-Synched**
4 **Chrome Users is a Serious Invasion of the Privacy and is Highly Offensive**

5 194. Chrome is now the most widely used browser in the world and is used by 59 percent
6 of all desktop computers in the United States.¹⁹

7 195. Article I, § 1 of the California Constitution provides: “All people are by nature free
8 and independent and have inalienable rights. Among these are enjoying and defending life and
9 liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety,
10 happiness, *and privacy*.” The phrase “*and privacy*” was added by the “Privacy Initiative” adopted
11 by California voters in 1972.

12 196. The right to privacy in California’s constitution creates a right of action against
13 private as well as government entities.

14 197. The principal purpose of this constitutional right was to protect against unnecessary
15 information gathering, use and dissemination by public and private entities, including computer-
16 stored and generated dossiers and cradle-to-grave profiles on every American.

17 198. In its public statements, Google pays lip-service to the need to protect the privacy
18 of Internet communications. For example, On June 6, 2016, a coalition of technology companies
19 and privacy advocates came together to oppose Congressional efforts to expand government
20 surveillance of online activities through the Senate’s Intelligence Authorization Act for Fiscal Year
21 2017 and Senator Cornyn’s proposed amendments to the ECPA.

22 199. The joint letter, signed by the ACLU, Amnesty International and others *was also*
23 *signed by Google*. These organizations and companies argued (correctly) that obtaining sensitive
24 information about Americans’ online activities without court oversight was an unacceptable
25 privacy harm because it “would paint an incredibly intimate picture of an individual’s life” if it

26 _____
27 ¹⁹ *Browser Market Share United States of America: May 2019 – May 2020*, GlobalStats,
28 <https://gs.statcounter.com/browser-market-share/all/united-states-of-america> (last visited June 19, 2020).

1 included “browsing history, email metadata, location information, and the exact date and time a
2 person signs in or out of a particular online account.”

3 200. The letter further posited that the proposed online surveillance could “reveal details
4 about a person’s political affiliations, medical conditions, religion, substance abuse history, sexual
5 orientation” and even physical movements. The letter concluded that online surveillance raises
6 “civil liberties and human rights concerns.”

7 201. Google has also publicly declared that non-consensual electronic surveillance is
8 “dishonest” behavior. For example, earlier this month, Google announced an update to its
9 “Enabling Dishonest Behavior Policy” (effective August 11, 2020) restricting advertising for
10 spyware and surveillance technology. The new policy, without any hint of irony, will now “prohibit
11 the promotion of products or services that are marketed or targeted with the express purpose of
12 tracking or monitoring another person or their activities without their authorization.”

13 202. Through this new amendment to Google’s pre-existing policy, Google now
14 explicitly takes the position that nonconsensual surveillance of “browsing history” is “dishonest
15 behavior.”

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

24 204. All three of these documents confirm that privacy is a human right and a violation
25 of privacy rights is a violation of human rights.

26 205. For example, the Universal Declaration declares that no one should be subject to
27 arbitrary interference with privacy, and even declares the right to the protection of laws against
28 such interference.

1 206. Similarly, the UN Guiding Principles for business identify privacy as a human right.

2 207. The third document, the GNI Principles, has an entire section dedicated to privacy
3 that begins: “Privacy is a human right and guarantor of human dignity. Privacy is important to
4 maintaining personal security, protecting identity and promoting freedom of expression in the
5 digital age.”

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

9 **I. Plaintiffs’ PI Is Property Owned by the Plaintiffs and Has Economic Value**

10 209. The value of personal data is well understood and generally accepted as a form of
11 currency.

12 210. It is by now incontrovertible that a robust market for this data undergirds the tech
13 economy.

14 211. The robust market for user data has been analogized to the “oil” of the tech
15 industry.²⁰ A 2015 article from TechCrunch accurately noted that “Data has become a strategic
16 asset that allows companies to acquire or maintain a competitive edge.”²¹ That article noted that
17 the value of a single Internet user—or really, a single user’s data—varied from about \$15 to more
18 than \$40.

19 212. The Organization for Economic Cooperation and Development (“OECD”) itself has
20 published numerous volumes discussing how to value data such as that which is the subject matter
21 of this Complaint, including as early as 2013, with its publication “Exploring the Economic of
22
23
24

25 ²⁰ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017),
26 <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

27 ²¹ Pauline Glickman and Nicolas Glady, *What’s the Value of Your Data?* TechCrunch (Oct. 13,
28 2015), <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>.

1 Personal Data: A Survey of Methodologies for Measuring Monetary Value”.²² The OECD
 2 recognizes that data is a key competitive input not only in the digital economy but in all markets:
 3 “Big data now represents a core economic asset that can create significant competitive advantage
 4 for firms and drive innovation and growth.”²³

5 213. In *The Age of Surveillance Capitalism*, Harvard Business School Professor
 6 Shoshanna Zuboff notes Google’s early success monetizing user data prompted large corporations
 7 like Verizon, AT&T and Comcast to transform their business models from fee for services provided
 8 to customers to monetizing their user’s data—including user data that is not necessary for product
 9 or service use, which she refers to as “behavioral surplus.”²⁴ In essence, Professor Zuboff explains
 10 that revenue from user data pervades every economic transaction in the modern economy. It is a
 11 fundamental assumption of these revenues that there is a *market* for this data; data generated by
 12 users on Google’s platform has economic value.

13 214. This is old news. In 2012, Google’s Chief Economist Hal Varian, in conversation
 14 with the *Economist*, referred to one aspect of data’s value as “nowcasting,” or “contemporaneous
 15 forecasting”—basically an ability to predict what is happening as it actually occurs.”²⁵ This kind
 16 of information clearly has economic value.

17 215. Professor Paul M. Schwartz writing in the Harvard Law Review, notes:

18 Personal information is an important currency in the new
 19 millennium. The monetary value of personal data is large and still
 20 growing, and corporate America is moving quickly to profit from the
 21 trend. Companies view this information as a corporate asset and have
 invested heavily in software that facilitates the collection of
 consumer information.

22 ²² *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary*
 23 *Value*, OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013),
<http://dx.doi.org/10.1787/5k486qtxldmq-en>.

24 ²³ *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct. 13,
 25 2013), https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en.

26 ²⁴ Shoshanna Zuboff, *The Age of Surveillance Capitalism* 166 (2019).

27 ²⁵ K.N.C., *Questioning the searches*, *The Economist* (June 13, 2012),
 28 <https://www.economist.com/schumpeter/2012/06/13/questioning-the-searchers>.

1 216. This economic value has been leveraged largely by corporations who pioneered the
 2 methods of its extraction, analysis, and use. However, the data also has economic value to users.
 3 Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize
 4 their own data. For example, Nielsen Data and Mobile Computer will pay users for their data.²⁶
 5 Google itself has launched apps that pay users for their data directly.²⁷ Likewise, apps such as Zynn,
 6 a TikTok competitor, pay users for to sign up and interact with the app.²⁸

7 217. There are countless examples of this kind of market, which is growing more robust
 8 as information asymmetries are diminished through revelations to users as to how their data is being
 9 collected and used.

10 218. Indeed, Google once paid users for the very data it now improperly harvests from
 11 Chrome:

12 Google is building an opt-in user panel that will track and analyze
 13 people's online behaviors via an extension to its Chrome browser,
 14 called Screenwise. Users that install the plug-in will have the
 15 websites they visit and the ways in which they interact with them
 16 recorded, and they will then be paid with Amazon gift cards worth
 17 up to \$25 a year in return.²⁹

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

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

22 ²⁶ Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (June 10,
 23 2020), <https://wallethacks.com/apps-for-selling-your-data/>.

24 ²⁷ Kari Paul, *Google launches app that will pay users for their data*, The Guardian (June 11, 2019),
 25 <https://www.theguardian.com/technology/2019/jun/11/Google-user-data-app-privacy-study>;
 26 Saheli Roy Choudhury and Ryan Browne, *Google pays teens to install an app that could collect all
 27 kinds of data*, CNBC (Jan. 30, 2019), [https://www.cnbc.com/2019/01/29/Google-paying-users-to-
 28 install-app-to-collect-data-techcrunch.html](https://www.cnbc.com/2019/01/29/Google-paying-users-to-install-app-to-collect-data-techcrunch.html); Tim Bradshaw, *Google offers to pay users for their
 voice recordings*, Financial Times (Feb. 21, 2020), [https://www.ft.com/content/42f6b93c-54a4-
 11ea-8841-482eed0038b1](https://www.ft.com/content/42f6b93c-54a4-11ea-8841-482eed0038b1).

²⁸ Jacob Kastrenakes, *A New TikTok Clone hit the top of the App Store by Paying users to watch
 videos*, The Verge (May 29, 2020), [https://www.theverge.com/2020/5/29/21274994/zynn-tiktok-
 clone-pay-watch-videos-kuaishou-bytedance-rival](https://www.theverge.com/2020/5/29/21274994/zynn-tiktok-clone-pay-watch-videos-kuaishou-bytedance-rival).

²⁹ Jack Marshall, *Google Pays Users for Browsing Data*, DigiDay (Feb. 10, 2012),
<https://digiday.com/media/google-pays-users-for-browsing-data/>.

age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.³⁰

220. There also a private market for users' personal information. One study by content marketing agency Fractl has found that an individual's online identity, including hacked financial accounts, can be sold for \$1,200 on the dark web.³¹ These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other users' content, surely users can sell their own. In short, there is economic value to users' data that is greater than zero. The exact number will be a matter for experts to determine.

J. Plaintiffs Have Suffered Economic Injury

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

222. Personal Information, including websites visited by the Plaintiffs, is property under California law.

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

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

225. Plaintiffs also have suffered benefit of the bargain damages, in that Google took more data than the parties agreed would be exchanged. Those benefit of the bargain damages also

³⁰ Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Literature 2, at 444 (June 2016), <https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf>.

³¹ Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*, MarketWatch (June 6, 2018), <https://www.marketwatch.com/story/spooked-by-the-google-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20>.

1 include, but are not limited to, (i) loss of the promised benefits of their Chrome experience; (ii) out-
2 of-pocket costs; and (iii) loss of control over property which has marketable value.

3 226. In addition, when Plaintiffs became Chrome users, they gained access to Chrome's
4 browser in exchange for agreeing to terms of service that Chrome drafted and sharing a limited
5 amount of data reflecting users' activity on the platform. In other words, those terms of service
6 assured users that data would not be sent to Google which was intended to, and did, encourage
7 Plaintiffs to engage more than they would have otherwise. The delta in data between what Chrome
8 promised and what in fact Chrome sent to Google can be measured in data and also in dollars,
9 because data has value.

10 227. Data brokers and online marketers have developed sophisticated schemes for
11 assessing the value of certain kinds of data, as discussed above. Experts in the field have identified
12 specific values to assign to certain kinds of activity. While Plaintiffs largely knew that Google
13 generates revenue from business by selling advertising directed at users, it was a material term of
14 the bargain that Plaintiffs' personal information would not be shared with Google if users did not
15 take the affirmative step of activating Sync for their Chrome account. It was also a material term
16 of the bargain that user would not "need to provide any personal information to use Chrome."

17 228. Google did not honor the terms of this bargain. Although the Chrome Privacy Notice
18 stated that Plaintiffs' did not "need to provide any personal information to use Chrome" and that
19 their personal information would not be shared with Google unless they Sync'd their account, in
20 practice, their information was shared with Google as if they had activated Sync.

21 229. When Chrome shared and Google collected Plaintiffs' personal information from
22 Chrome that Plaintiffs had not chosen to share with Google, Google received benefits. First, Google
23 captured-revenues associated with increased user activity on the Chrome browser and from
24 enhanced targeting as a result of ever-more detailed datasets collected about users. Second, Google
25 also transferred costs and harms to Plaintiffs in that Google did not have to invest in protecting that
26 data or preventing its dissemination as it promised users it would.

27 230. As Google expanded the scope of access to Plaintiffs' personal information beyond
28 that which Plaintiffs had agreed, users were denied the benefit of a Chrome experience where they

1 were promised the right to determine the terms and scope of their content and personal information
2 sharing. Thus, through Chrome’s sharing of Plaintiffs’ personal information with Google, Plaintiffs
3 lost benefits.

4 231. In order to preserve their privacy, Plaintiffs who now understand at least some of
5 Google’s violations—and there is much to be revealed about Google’s actual activities—are
6 presented with the choice of: (i) reducing or ending their participation on Chrome; or (ii) knowingly
7 accepting less privacy than that which was promised. Each of these options deprives Plaintiffs of
8 the remaining benefits of their original bargain. There is no option which recovers it. None of it
9 recaptures the data taken in violation of Chrome’s promises.

10 232. Further, Plaintiffs were denied the benefit of this information and therefore the
11 ability to mitigate harms they incurred because of Chrome’s impermissible disclosure of their
12 personal information to Google. That is, Google’s lack of transparency prevented and still prevents
13 Plaintiffs’ ability to mitigate.

14 233. Google knew that it was collecting users’ personal information regardless of
15 whether users had taken affirmative steps to turn on the synchronization feature. Yet, Google failed
16 to warn users so that they could take steps to avoid exposing their information on Chrome.

17 234. Google also knew that it was not possible for users to use Chrome without providing
18 any personal information.

19 235. Google avoided costs it should have incurred because of its own actions—
20 particularly the loss of user engagement which would have resulted from transparent disclosure of
21 Googler’s actions—and transferred those costs to Plaintiffs. Warning users would have chilled
22 Chrome engagement as well as discourage potential new users from joining.

23 236. Google was thus not only able to evade or defer these costs but to continue to accrue
24 value for the Company and to further benefit from the delay due to the time value of money. Google
25 has thus transferred all the costs imposed by the unauthorized disclosure users’ content and personal
26 information onto Plaintiffs. Google’s increased mitigation costs by failing to notify users that their
27 personal information had been disclosed and to alert them at the earliest time possible so that users
28 could take steps to minimize their exposure on the browser.

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

3 238. Plaintiffs' personal information has value. First, there is transactional, or barter,
4 value to user content and personal information. Indeed, Google has traded the ability to use its
5 Chrome browser for the collection of users' personal information—all the while promising users
6 that it was not necessary for them to share any personal information to use Chrome and that Chrome
7 would not share any of their personal information with Google unless they were Synched.

8 239. Second, Plaintiffs' property, which has economic value, was taken from them
9 without their consent and in contradiction of Chrome's express promise not to send it to Google.
10 There is a market for this data, and it has at minimum a value greater than zero.

11 240. Users were harmed when Google took their property and exerted exclusive control
12 over it, collecting it without users' knowledge and for still undisclosed purposes.

13 **K. Google Has Been Unjustly Enriched**

14 241. Google's \$1 trillion business was built entirely on monetizing the value of Internet
15 users' data.³²

16 242. Professor Zuboff details Google's role as one of the main drivers of data collection
17 and monetization:

18 In 2016, 89 percent of the revenues of [Google's] parent company,
19 Alphabet, derived from Google's targeted advertising programs. The
20 scale of raw-material flows is reflected in Google's domination of
21 the internet, processing over 40,000 search queries every second on
22 average: more than 3.5 billion searches per day and 1.2 trillion
23 searches per year worldwide in 2017.³³

24 243. Indeed, "Google maximizes the revenue it gets from [landing pages] by giving its
25 best position to the advertiser who is likely to pay Google the most in total, based on the price per
26

27 ³² *Google owner Alphabet is now worth \$1 trillion*, CNN (Jan. 16, 2020),
28 <https://www.cnn.com/2020/01/16/investing/google-trillion-dollar-market-value-apple-microsoft/index.html>.

³³ Zuboff, *supra*, at 92

1 click multiplied by Google’s estimate of the likelihood that someone will actually click on the
2 ad.”³⁴

3 244. For its part, Google explains under the header of “How we make money” in its
4 annual financial statements, that its goal is to “deliver relevant ads at just the right time and to give
5 people useful commercial information, regardless of the device they’re using.”³⁵ Google explains
6 further that its revenues are based primarily on the delivery of “performance advertising,” and
7 “brand advertising.”

8 245. Performance advertising, as Google explains, is driven by users’ engagement with
9 an advertisement and Google is paid by the advertiser when a user engages in the ad. Brand
10 advertising is built through “enhance[ing] users’ awareness of and affinity with advertisers’
11 products and services, through videos, text, images, and other interactive ads that run across various
12 devices.” Under both, Google’s revenues are built upon the ability to target users with
13 advertisements based upon the personal information that Google has collected.

14 246. The value of Chrome users’ personal information to Google is demonstrated in part
15 by Google’s advertisement revenue during the relevant time period. Google reported \$134.8 billion
16 in advertising revenue in 2019, \$116.4 billion in 2018, \$95.5 billion in 2017, and \$79.3 billion in
17 2016.³⁶ This translates to 83% of Google’s total revenues in 2019, 85% in 2018, 86% in 2017 and
18 87% in 2016.³⁷ While not all of that value is unjustly derived from the specific information collected
19 by Google here, some portion of it is.

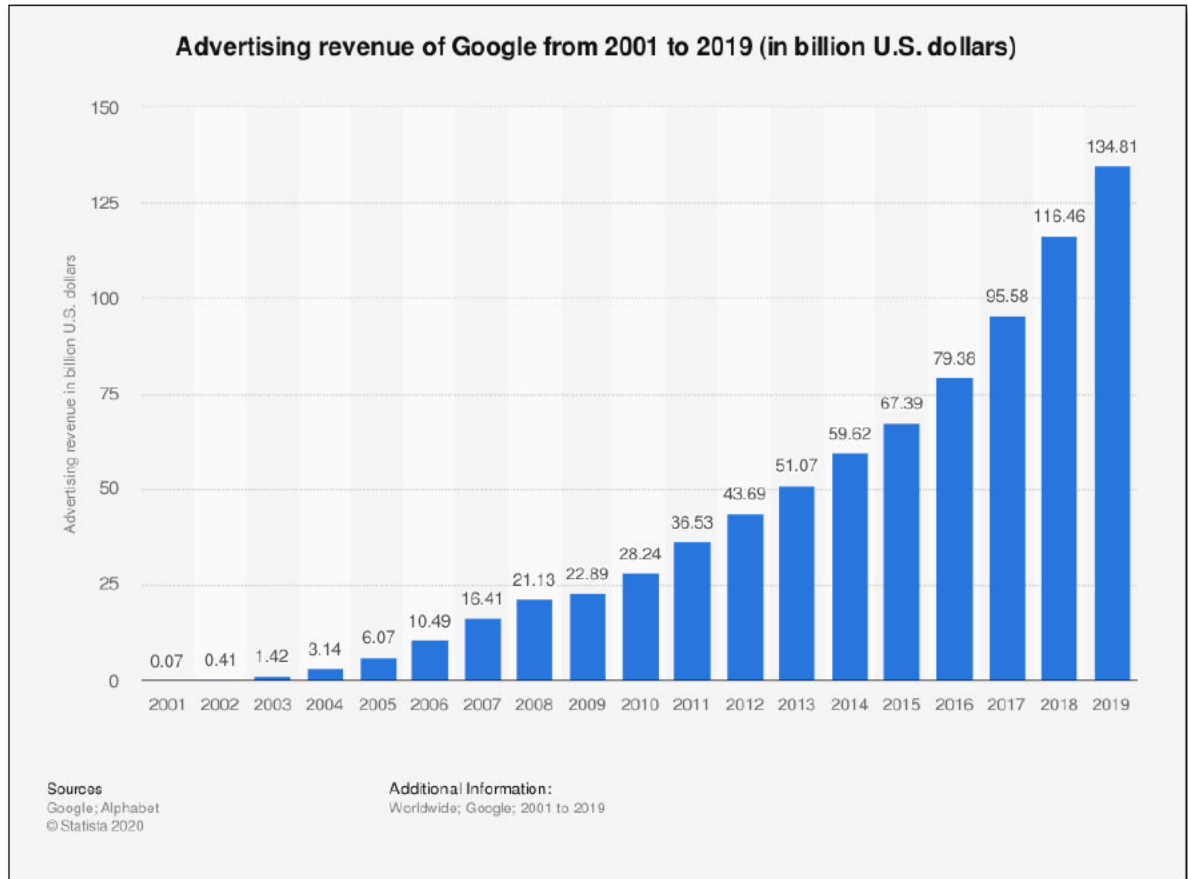
21 ³⁴ Peter Coy, *The Secret to Google’s Success*, Bloomberg (Mar. 6, 2006),
22 <http://www.bloomberg.com/news/articles/2006-03-05/the-secret-to-googles-success>.

23 ³⁵ *2019 Annual Report*, Alphabet Inc. (Feb. 3, 2020),
<https://www.sec.gov/ix?doc=/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm#sFA530FF828B154C8973614936FC32E93>.

24 ³⁶ *2019 Annual Report*, Alphabet Inc. (Feb. 3, 2020),
25 <https://www.sec.gov/ix?doc=/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm#sFA530FF828B154C8973614936FC32E93>; *2018 Annual Report*, Alphabet Inc.
26 (Feb. 4, 2019),
<https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm>.

27 ³⁷ 2019 Annual Report; 2018 Annual Report.

1 247. Shown graphically below, Google’s annual advertising revenue has increased over
2 five hundred percent since it first released Chrome in 2008.³⁸



17 248. Google’s increased revenue is driven in part by the increased engagement by users,
18 which Google quantifies as “paid clicks” across Google properties, including Chrome. According
19 to Google’s annual reports, Google has increased the number of its paid clicks by 23% in 2019,
20 62% in 2018, 70.5% in 2017, and 70.9% in 2016.

21 249. In addition to these metrics, estimates of Google average revenue per monthly active
22 user from advertising on its sites is \$6.70 in the fourth quarter of 2016.³⁹ Other estimates of the
23

24
25 ³⁸ J. Clement, *Advertising revenue of Google from 2001 to 2019*, statista (Feb. 5, 2020),
<https://www.statista.com/statistics/266249/advertising-revenue-of-google/>.

26 ³⁹ J. Clement, *Google’s average revenue per monthly active user from 1st quarter 2015 to 4th*
27 *quarter 2016*, statista (May 24, 2017), <https://www.statista.com/statistics/306570/google-annualized-advertising-arpu/>.

28

1 average revenue per user per year for Google place the value at \$256.⁴⁰ And at \$55 for digital
2 revenue per member.⁴¹

3 250. The collection of users' PI has also facilitated the revenues of Google's Network
4 Members' properties which include ads placed through AdMob, AdSense, DoubleClick
5 AdExchange. Google's Network Members' properties revenues increased by \$21.5 in 2019, \$20
6 billion in 2018, \$17.6 billion in 2017, and \$15.5 billion in 2016.⁴²

7 251. Google uses information collected from users to deliver targeted advertisements to
8 users across Google's services and across users' devices. The delivery of targeted advertisements
9 leads to more engagement with the advertisements, which allows Google to sell the advertisements
10 at a higher rate.

11 252. Google has recently disclosed the shared take rates from buying portals, Google Ads
12 and Display & Video 360, and from publisher services, Google Ad Manager. The disclosure show
13 that "when marketers used Google Ads or Display & Video 360 to buy display ads on Google Ad
14 Manager," Google keeps 31% of the ad spend.⁴³ Google's cut of the ad spend further demonstrates
15 the markup achieved by its collection, and use of users' personal information.

16 253. Google further quantifies the value of users' data through several user-based
17 metrics, including cost-per-impressions and cost-per-click. Google defines "cost-per-impressions"
18 for Google Network Members' properties, such as AdMob, AdSense, DoubleClick AdExchange,
19 as the "impression-based and click-based revenues divided by our total number of impressions and
20

21
22 _____
23 ⁴⁰ Frederic Filloux, *The ARPUs of the Big Four Dwarf Everybody Else*, Medium (Feb. 10, 2019),
<https://mondaynote.com/the-arpus-of-the-big-four-dwarf-everybody-else-e5b02a579ed3>.

24 ⁴¹ Frederic Filloux, *The NYTimes could be worth \$19bn instead of \$2bn*, Medium (Feb. 15, 2015),
<https://mondaynote.com/the-nytimes-could-be-worth-19bn-instead-of-2bn-8ab635bc6262>.

25 ⁴² 2019 Annual Report; 2018 Annual Report.

26 ⁴³ Sissie Hsiao, *How our display buying platforms share revenue with publishers*, Google Ad
27 Manager (June 23, 2020), <https://blog.google/products/admanager/display-buying-share-revenue-publishers/>.

28

1 represents the average amount we charge advertisers for each impression displayed to users.”⁴⁴

2 Google reported a 9% increase in cost-per-impressions for 2019, and 2% increase in 2018.

3 254. Google also reports the “cost-per-click,” which it defines as “click-driven revenues
4 divided by our total number of paid clicks and represents the average amount we charge advertisers
5 for each engagement by users.”⁴⁵ Google does not include the actual cost-per-click in financial
6 reports. However, the average costs per click on Google Ads is reportedly \$2.32.⁴⁶

7 255. Google’s user-based revenues are driven by its collection of Internet users’
8 information to create detailed dossiers about individual’s personal information, including names,
9 address, education, income, hobbies, interests, relationships, politics, religious beliefs, and more.

10 256. Although Google promises that Chrome users can opt out of Google surveillance by
11 not providing any personal information to use Chrome and not Syncing their data, those promises
12 are not true. And Chrome plays a large part, with over 2 billion active installs allowing data
13 generation and extraction trillions of times on a daily basis.⁴⁷

14 257. Unbeknownst to users, Google has programmed Chrome for surveillance no matter
15 what the user does. By encouraging engagement with Chrome with its promise not to share data
16 with Google, Google ensures that it will be able to track an ever-larger percentage of Internet users.

17 258. In other words, Chrome’s promise not to send Un-Synced users’ PI to Google was
18 intended to (and did) stimulate greater user engagement. Those false promises also prevented
19 decreased user engagement by disclosing what Chrome’s actual practices are. And Google directly
20 profited from that increased user engagement.

21
22
23 ⁴⁴ 2019 Annual Report.

24 ⁴⁵ *Id.*

25 ⁴⁶ Dan Shewan, *The Comprehensive Guide to Online Advertising Costs*, WordStream
26 (Apr. 20, 2020), <https://www.wordstream.com/blog/ws/2017/07/05/online-advertising-costs#:~:text=The%20average%20cost%20of%20an,18..>

27 ⁴⁷ Frederic Lardinois, *Google says there are now 2 billion active Chrome installs*, TechCrunch
28 (Nov. 10, 2016), <https://techcrunch.com/2016/11/10/google-says-there-are-now-2-billion-active-chrome-installs/>.

VI. CLASS ACTION ALLEGATIONS

1 259. This is a class action pursuant to Rules 23(a) and (b)(3) (or, alternatively, 23(c)(4))
2 of the Federal Rules of Civil Procedure on behalf of a Class of all persons residing in the United
3 States who used Google’s Chrome browser on or after July 27, 2016 without choosing to Sync with
4 any Google account and whose personal information was collected by Google.

5 260. Excluded from the Class are the Court, Defendants and their officers, directors,
6 employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in
7 which any of them have a controlling interest.

8 261. The members of the Class are so numerous that joinder of all members is
9 impracticable.

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

- 13 a. Whether Chrome shares user personal information with Google when users
14 were not Synched with their Google accounts;
- 15 b. Whether Chrome users can use the service without providing personal
16 information to Chrome;
- 17 c. Whether Google had authorization from Un-Synched Chrome Users to
18 disclose the content of user communications while in storage on the Chrome
19 browser;
- 20 d. Whether Google had user authorization from Un-Synched Chrome Users to
21 disclose the content of user communications contemporaneous to their
22 making;
- 23 e. Whether Google had user authorization from Un-Synched Chrome Users to
24 acquire the content of user communications while they were in storage in the
25 Chrome browser;
- 26
- 27
- 28

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

- f. Whether Google had user authorization from Un-Synched Chrome Users to acquire the content of user communications contemporaneous to their making;
- g. Whether Google’s actions to disclose and acquire the contents of Un-Synched Chrome User communications violate the federal Electronic Communications Privacy Act;
- h. Whether Google’s actions violate the California Invasion of Privacy Act;
- i. Whether Google breached its contract with Un-Synched Chrome Users;
- j. Whether the Personal Information improperly collected by Google from the Un-Synched Users has economic value; and
- k. Whether Google unjustly profited from the improperly collected Personal Information of the Un-Synched Chrome Users.

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

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

265. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages individual Class and Subclass members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class and Subclass to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

VII. COUNTS

COUNT ONE

**WIRETAP ACT: UNAUTHORIZED INTERCEPTION
OF ELECTRONIC COMMUNICATIONS
18 U.S.C. § 2510, et seq.**

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

267. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional interception of the contents any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

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

269. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

270. Google intentionally intercepted the electronic communications of Plaintiffs and other Un-Synched Chrome Users.

271. The transmission of data between plaintiffs and the websites on which Google tracked and intercepted their communications without authorization while they were Un-Synched were “transfer[s] of signs, signals, writing, ... data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects interstate commerce[,]” and were therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(12).

272. Google’s interception of Plaintiffs’ communications was done contemporaneously with the Plaintiffs’ sending and receipt of those communications.

273. The intercepted communications include:

- a. The precise text of GET requests that Chrome users’ exchange with non-Google websites;
- b. The precise text of user search queries at non-Google sites;
- c. The precise text of specific buttons that users click to exchange communications at non-Google websites, such as “Log-In” or “Submit.”
- d. The precise text of information that users submit in forms to exchange

1 communications at non-Google websites.

2 e. Information that is a general summary or informs Google of the general
3 subject of communications that non-Google websites send back to users in
4 response to search queries and requests for information.

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

6 a. The cookies Google used to track the Plaintiffs’ communications while they
7 were not Synched with any Google account, including cookies Google sets
8 and acquires through other entities through cookie-synching;

9 b. The Plaintiffs’ browsers;

10 c. The Plaintiffs’ computing devices;

11 d. Google’s web servers;

12 e. The web-servers of websites from which Google tracked and intercepted the
13 Plaintiffs’ communications while they were not Synched with any Google
14 account; and

15 f. The computer code deployed by Google to effectuate its tracking and
16 interception of the Plaintiffs’ communications while not Synched with any
17 Google account.

18 275. Google is not a party to Plaintiffs’ electronic communications with non-Google
19 websites.

20 276. Google’s received the content of Plaintiff communications with non-Google
21 websites through the surreptitious duplication and forwarding of those communications by Chrome
22 to Google.

23 277. Plaintiffs were logged-off of Google Sync when Google intercepted the
24 communications at issue.

25 278. Plaintiffs did not consent to Google’s acquisition of the contents of their
26 communications with non-Google websites while using the Chrome browser when not logged-in
27 to Google Sync because Google expressly promised that “[t]he personal information that Chrome
28 stores [about users] won’t be sent to Google unless” the Chrome user “choose[s] to store that data

1 in” their “Google Account by turning on sync,” i.e. formally logging-in to a Google service called
2 Sync.

3 279. Google’s failure to adequately inform websites using its third-party tracking tools
4 that Google had promised Chrome users that it would not share user personal information unless
5 the user was logged-in to Sync constituted a fraud and mistake of fact that vitiates any alleged
6 consent that Google may claim for the non-Google websites.

7 280. The ECPA includes a separate affirmative defense for the officers, employees, and
8 agents of electronic communication service providers, whose facilities are used in the transmission
9 of electronic communications, “to intercept, disclose, or use that communication in the normal
10 course of his employment while engaged in any activity which is a necessary incident to the
11 rendition of his service or the protection of the rights or property of the provider of that service[.]”

12 281. As alleged herein, the Google services to which Chrome re-directs Chrome user
13 communications are not agents of Chrome.

14 282. The surreptitious re-direction of Chrome user communications to Google while the
15 users were not logged-in to Google Sync was not done in Chrome’s “normal course” and is not a
16 “necessary incident to the rendition” of electronic communication service.

17 283. The surreptitious re-direction of Chrome user communications to Google while
18 users were not logged-in to Google Sync was not done for “the protection of the rights or property”
19 of Chrome, but instead for advertising and surveillance purposes by Google’s other services.

20 284. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may
21 assess statutory damages to Plaintiffs; injunctive and declaratory relief; punitive damages in an
22 amount to be determined by a jury, but sufficient to prevent the same or similar conduct by
23 Defendant in the future, and a reasonable attorney’s fee and other litigation costs reasonably
24 incurred.

25
26
27
28

COUNT TWO

WIRETAP ACT – UNAUTHORIZED DISCLOSURES BY AN ECS
18 U.S.C. § 2510, et. seq.

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

285. The Electronic Communications Privacy Act provides that “a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.” 18 U.S.C. § 2511(3)(a).

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

287. Google Chrome is an ECS because it provides to users thereof the ability to send or receive electronic communications.

288. In the absence of a web-browser, Internet users could not send or receive communications over the Internet.

289. Chrome is an ECS provided to the public.

290. Chrome intentionally divulged the contents of user communications with non-Google websites to Google while those user communications were in transmission on Chrome.

291. Google was not an addressee or intended recipient of Plaintiffs’ communications on Chrome while they were not logged-in to Google Sync.

292. Google was not an addressee or intended recipient of the non-Google websites communications to Plaintiffs’ using Chrome while they were not logged-in to Google Sync.

293. Google was not an agent of the Plaintiffs or the non-Google websites.

294. The ECPA provides that “a person or entity providing an [ECS] to the public may divulge the contents of any such communication—(i) as otherwise authorized in sections 2511(2)(a) or 2517 of this title;” (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are

1 used, to forward such communication to its destination; (iv) which were inadvertently obtained by
2 the service provider and which appear to pertain to the commission of a crime, if such divulgence
3 is made to a law enforcement agency.”

4 295. Section 2511(2)(a) exempts the contents of communications divulged to “an officer,
5 employee, or agent” of an ECS “in the normal course of employment ... while engaged in any
6 activity which is a necessary incident to the rendition” of service “or to the protection of the rights
7 or property of the provider of that service[.]” Google lacks this affirmative defense because
8 Chrome’s divulgences to Google Doubleclick, Google Analytics, Google Ads, and other Google
9 divisions was not “in the normal course” of the provision of ECS, was not a “necessary incident to
10 the rendition” of ECS service, and was not for “the protection of the rights or property” of Google.
11 Instead, the divulgences were for Google’s advertising and surveillance purposes.

12 296. Section 2517 relates to divulgences to law enforcement officers and is not pertinent
13 here.

14 297. Chrome lacks the “lawful consent” of the originator and any addressee or intended
15 recipients of the relevant communications because:

- 16 a. Chrome expressly promised its ECS users that their personal information,
17 including the contents of their browsing communications, would not be
18 shared with Google unless the user was logged-in to Google Sync;
- 19 b. Chrome and Google failed to inform non-Google websites using Google
20 third-party tracking source code that Chrome promised its users not to
21 divulge such information; and
- 22 c. Chrome failed to block divulgences of Chrome user communications to
23 Google advertising entities when users were not logged-in to Google Sync,
24 despite having promised to not share such information with Google in
25 those circumstances.

26 298. The Google advertising entities to which the contents of Chrome users’
27 communications were divulged are not employed or authorized, and do not have facilities used, to
28 forward user communications to their intended destinations.

1 299. The affirmative defines for disclosures to law enforcement does not apply.

2 300. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may
3 assess statutory damages to Plaintiffs; injunctive and declaratory relief; punitive damages in an
4 amount to be determined by a jury, but sufficient to prevent the same or similar conduct by
5 Defendant in the future, and a reasonable attorney’s fee and other litigation costs reasonably
6 incurred.

7
8 **COUNT THREE**

9 **STORED COMMUNICATIONS ACT – UNAUTHORIZED**
10 **ACCESS TO STORED ECS COMMUNICATIONS**
11 **18 U.S.C. § 2701**

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

13 302. The Stored Communications Act (“SCA”) provides a cause of action against a
14 person who “intentionally accesses without authorization a facility through which an electronic
15 communication service is provided” or “who intentionally exceeds an authorization to access that
16 facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic
17 communication while it is in electronic storage in such a system.” 18 U.S.C. § 2701(a).

18 303. As set forth above, Google Chrome is an ECS. Google has explained that a web
19 browser is where Internet users “search, chat, email, and collaborate,” and, “in our spare time, we
20 shop, bank, read news, and keep in touch with friends – all using a browser.”

21 304. The ECPA does not provide a separate definition for “facility” but instead it is
22 defined within the context of the sentences in which it is used.

23 305. A “facility” under the ECPA is, under the plain language of the statute, that “through
24 which an electronic communication service is provided.” 18 U.S.C. § 2701(a).

25 306. The ECPA also uses the term “facility” when describing the facts necessary to
26 support a law enforcement application for a Wiretap order, which “shall include,” among other
27 things “a particular description of the nature and location of the facilities from which or the place
28 where the communication is to be intercepted.” 18 U.S.C. § 2518(1)(b). As used in this ECPA

1 section, “facility” has included telephones and other communications devices that officers have
2 formally requested to be tapped.

3 307. The items through which the electronic communication services of the Chrome web-
4 browser include:

- 5 a. The Plaintiffs’ personal computing devices;
- 6 b. The Plaintiffs’ Chrome browsers;
- 7 c. The browser-managed files which, together, constitute all of the programs
8 contained within the Plaintiffs’ Chrome browsers; and
- 9 d. Plaintiffs’ IP addresses.

10 308. Google intentionally accessed the Plaintiffs’ personal computing devices, Chrome
11 browsers, browser-managed files, and IP addresses via the Chrome browser while the Plaintiffs
12 were not logged-in to Google Sync.

13 309. Plaintiffs did not authorize Google to access the content of their communications
14 stored on their personal computers and the Chrome browser while they were not logged-in to
15 Google Sync.

16 310. The information obtained by Google through its unauthorized access included
17 “contents” as described above

18 311. The ECPA defines “electronic storage” as “any temporary, intermediate storage of
19 a wire or electronic communication incidental to the electronic transmission thereof;” and “any
20 storage of such communication by an electronic communication service for purposes of backup
21 protection of such communication.” 18 U.S.C. § 2510(17).

22 312. Chrome stores the contents of user communications immediately upon a user’s
23 sending of any communication in at least two ways:

- 24 a. For purposes of backup protection so that if the browser inadvertently shuts
25 down, the user can be presented with the option to restore previous
26 communications; and
- 27 b. For a temporary and intermediate amount of time incidental to the
28 electronic transmission thereof when it places the contents of user

1 communications into the browser’s web-browsing history, which is only
2 kept on the browser for 90 days.

3 313. Plaintiffs and Class Members were harmed by Google’s actions, and pursuant to 18
4 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Google attributable to
5 the violations or statutory minimum damages of \$1,000 per plaintiff, punitive damages, costs, and
6 reasonable attorney’s fees.

7
8 **COUNT FOUR**

9 **STORED COMMUNICATIONS ACT – UNAUTHORIZED**
10 **DISCLOSURES OF STORED COMMUNICATIONS BY AN ECS**
11 **18 U.S.C. § 2701**

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

13 315. The ECPA provides that “a person or entity providing an electronic communication
14 service to the public shall not knowingly divulge to any person or entity the contents of a
15 communication while in electronic storage by that service.”

16 316. As alleged above, Google Chrome is an ECS to the public.

17 317. As alleged above, Chrome knowingly divulges the contents of user communications
18 to Google while those user communications are in electronic storage by Chrome.

19 318. Plaintiffs and Class Members were harmed by Google’s actions, and pursuant to
20 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Google attributable
21 to the violations or statutory minimum damages of \$1,000 per plaintiff, punitive damages, costs,
22 and reasonable attorney’s fees.

23 **COUNT FIVE**

24 **VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (“CIPA”)**
25 **Cal. Penal Code §§ 631**

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

27 320. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638.
28 The Act begins with its statement of purpose:

The Legislature hereby declares that advances in science and
technology have led to the development of new devices and

1 techniques for the purpose of eavesdropping upon private
2 communications and that the invasion of privacy resulting from the
3 continual and increasing use of such devices and techniques has
4 created a serious threat to the free exercise of personal liberties and
5 cannot be tolerated in a free and civilized society.

6 Cal. Penal Code § 630.

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

8 Any person who, by means of any machine, instrument, or
9 contrivance, or in any other mannerwillfully and without the
10 consent of all parties to the communication, or in any unauthorized
11 manner, reads, or attempts to read, or to learn the contents or meaning
12 of any message, report, or communication while the same is in transit
13 or passing over any wire, line, or cable, or is being sent from, or
14 received at any place within this state; or who uses, or attempts to
15 use, in any manner, or for any purpose, or to communicate in any
16 way, any information so obtained, or who aids, agrees with, employs,
17 or conspires with any person or persons to lawfully do, or permit, or
18 cause to be done any of the acts or things mentioned above in this
19 section, is punishable by a fine not exceeding two thousand five
20 hundred dollars ...

21 322. Google is a “person” or “persons” within the meaning of § 631(a).

22 323. Under § 631, a defendant must show it had the consent of all parties to a
23 communication.

24 324. Google is headquartered in California; designed and contrived and effectuated its
25 scheme to track its users while not logged-in to Sync in California; and has adopted California
26 substantive law to govern its relationship with its users.

27 325. At all relevant times, Google’s tracking and interceptions of the Plaintiffs’ Internet
28 communications while not logged-in to Sync was without authorization and consent from the
Plaintiffs.

326. Google’s non-consensual tracking of logged-out users’ Internet browsing was
designed to learn or attempt to learn the meaning of the contents of Chrome users’ communications.

327. Chrome aided and abetted Google in its learning or attempting to learn the meaning
of the contents of Chrome users’ communications.

328. The following items constitute “machine[s], instrument[s], or contrivance[s]” under
the CIPA, and even if they do not, Google’s deliberate and admittedly purposeful scheme that
facilitated its interceptions falls under the broad statutory catch-all category of “any other manner”:

- 1 a. The cookies Google used to track the Plaintiffs' communications while they
- 2 were not logged-in to Google Sync;
- 3 b. The Plaintiffs' browsers;
- 4 c. The Plaintiffs' personal computing devices;
- 5 d. Google's web servers;
- 6 e. The web-servers of non-Google websites from which Google tracked and
- 7 intercepted the Plaintiffs' communications while they were not logged-in to
- 8 Google Sync; and
- 9 f. The computer code Google deployed to effectuate its tracking and
- 10 interception of the Plaintiffs' communications while Plaintiffs were not
- 11 logged-in to Google Sync;
- 12 g. The plan Google carried out to achieve its tracking and interception of the
- 13 Plaintiffs' communications while they were not logged-in to Google Sync.

14 329. Google's learning or attempts to learn the contents of Plaintiffs' communications
15 while not logged-in to Google Sync occurred while Plaintiffs' communications with non-Google
16 websites were in transit or in the process of being sent or received.

17 330. Plaintiffs and Class Members have suffered loss by reason of these violations,
18 including, but not limited to, violation of their rights to privacy and loss of value in their PI.

19 331. Pursuant to Cal. Pen. Code § 637.2, Plaintiffs and the Class have been injured by
20 Defendant's violations of Cal. Pen. Code § 631 and each seek damages for the greater of \$5,000 or
21 three times the amount of actual damages, as well as injunctive relief.

22 **COUNT SIX**

23 **INVASION OF PRIVACY**

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

25 333. Google has intruded upon the following legally protected privacy interests of
26 Plaintiffs:

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

- 1 b. A right to be free from Internet surveillance absent consent;
- 2 c. Statutory rights codified in federal and California privacy statutes;
- 3 d. The California Computer Crime Law, Cal Pen. Code § 502, which applies to
- 4 all plaintiffs in this case by virtue of Google’s choice of California law to
- 5 govern its relationship with Google users;
- 6 e. Cal. Penal Code § 484(a) which prohibiting the knowing theft or defrauding
- 7 of property “by any false or fraudulent representation or pretense[.]”

8 334. The Google Terms of Service, and other public promises Google made not to track
9 or intercept the Plaintiffs’ communications or access their computing devices and Chrome browsers
10 while not Synched with any Google accounts.

11 335. Plaintiffs had a reasonable expectation of privacy in the circumstances in that:
12 a. Plaintiffs could not reasonably expect Google would commit acts in violation
13 of federal and state laws;

14 b. Google affirmatively promised users it would not cause Chrome to send their
15 personal information to Google unless the users choose to Sync with their
16 Google accounts

17 336. Google’s actions constituted a serious invasion of privacy in that they:
18 a. Invaded a zone of privacy protected by the Fourth Amendment, namely the
19 right to privacy in data contained on personal computing devices, including
20 web search and browsing histories;

21 b. Violated several federal criminal laws, including the Wiretap Act, and Stored
22 Communications Act;

23 c. Violated dozens of state criminal laws;

24 d. Invaded the privacy rights of hundreds of millions of Americans without their
25 consent;

26 e. Constituted the unauthorized taking of valuable information from hundreds
27 of millions of Americans through deceit.

28

1 337. The surreptitious and unauthorized tracking of the internet communications and
2 associated personal information of millions of Americans’ constitutes an egregious breach of social
3 norms.

4 338. Google lacked a legitimate business interest in tracking users without consent.

5 339. Plaintiffs have been damaged by Google’s invasion of their privacy and are entitled
6 to just compensation.

7
8 **COUNT SEVEN**

9 **INTRUSION UPON SECLUSION**

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

11 341. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into
12 a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

13 342. In carrying out its scheme to track and intercept Plaintiffs’ communications and
14 access their computing devices and Chrome browsers while they were not Synched with other
15 Google accounts in violation of the governing Terms of Service, Google intentionally intruded
16 upon the Plaintiffs’ solitude or seclusion in that it effectively placed itself in the middle of
17 communications to which it was not an authorized party and acquired data that was private and
18 Google was not authorized to acquire.

19 343. Google’s actions were not authorized by the Plaintiffs nor by the websites with
20 which they were communicating.

21 344. Defendant’s intentional intrusion into Plaintiffs’ Internet communications and their
22 computing devices and Chrome browsers was highly offensive to a reasonable person in that they
23 violated federal and state criminal and civil laws designed to protect individual privacy and against
24 theft.

25 345. The unauthorized disclosure and taking of personal information from hundreds of
26 millions of Americans through deceit is highly offensive behavior.

27 346. Secret monitoring of web browsing is highly offensive behavior.
28

1 347. Wiretapping and surreptitious recording of communications is highly offensive
2 behavior.

3 348. Public polling on Internet tracking has consistently revealed that the overwhelming
4 majority of Americans believe it is important or very important to be “in control of who can get
5 information” about them; to not be tracked without their consent; and to be in “control[] of what
6 information is collected about [them].”⁴⁸

7 349. Plaintiffs have been damaged by Google’s invasion of their privacy and are entitled
8 to reasonable compensation including but not limited to disgorgement of profits related to the
9 unlawful internet tracking.

10 **COUNT EIGHT**

11 **BREACH OF CONTRACT**

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

13 351. Google’s relationship with its users is governed by the Google general Terms of
14 Service, Chrome TOS and Chrome Privacy Notice, current and prior versions of which are attached
15 to this Complaint as Exhibits 2 through 33.

16 352. Google promised that Chrome would not report PI to Google unless the Plaintiffs
17 affirmatively chose to Sync the browser with their Google accounts.

18 353. Google breached this promise.

19 354. Plaintiffs fulfilled their obligations under the relevant contracts and are not in breach
20 of any.

21 355. As a result of Google’s breach, Google was able to obtain the personal property of
22 Plaintiffs and other Un-Synched Chrome Users, earn unjust profits, and caused privacy injury and
23 other consequential damages.

24
25
26
27 ⁴⁸ Auxier and Rainie, “Key takeaways on Americans’ views about privacy, surveillance and data-
28 sharing” [https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-
about-privacy-surveillance-and-data-sharing/](https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/) (last accessed July 23, 2020).

1 in the form of their personal information, which, as alleged above, has ascertainable value to be
2 proven at trial.

3 **COUNT TEN**

4 **QUASI-CONTRACT (RESTITUTION AND UNJUST ENRICHMENT)**
5 **(IN ALTERNATIVE TO CONTRACT CLAIMS)**

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

7 368. Defendant, intentionally and without consent or other legal justification, violated the
8 privacy, property, and statutory rights of Plaintiffs and other Un-Synched Chrome Users.

9 369. As a result of Defendant's tortious acts, Defendant received and unjustly retained a
10 benefit at the expense of Plaintiffs and other Un-Synched Chrome Users.

11 370. It would be unjust for Defendant to retain the value of the Plaintiffs' property and
12 any profits earned thereon.

13 371. If Plaintiffs' contract claims fail they have no adequate remedy at law to force the
14 disgorgement of Defendant's unjustly earned profits. This count is therefore pled in the alternative
15 to the contract claims.

16 **COUNT ELEVEN**

17 **VIOLATION OF COMPUTER FRAUD AND ABUSE ACT ("CFAA")**
18 **18 U.S.C. §1030(g)**

19 372. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

20 373. The CFAA prohibits the knowing "transmission of a program, information, code or
21 command, and as a result of such conduct, intentionally causes damage without authorization, to a
22 protected computer." 18 U.S.C. § 1030(a)(5)(A).

23 374. The Plaintiffs' computers are "protected computers" within the meaning of the
24 statute.

25 375. The Chrome browser was represented to protect user privacy (by blocking the
26 transmission of PI to Google) unless the user affirmatively elected to Sync the browser with other
27 Google accounts.

28 376. Chrome's purported ability to protect user privacy was a core feature of Chrome.

1 377. Google transmitted code to the Plaintiffs' computers that caused Chrome to transmit
2 PI to Google without Plaintiff's authorization.

3 378. The CFAA defines "damage" to mean "impairment to the integrity or availability of
4 data, a program, a system or information."

5 379. Google's unauthorized actions impaired the integrity of Plaintiffs' data, browsers
6 and computer systems by removing a key privacy feature that should have blocked Google's
7 surveillance.

8 380. The CFAA provides a private right of action by any person who suffers damage or
9 loss as a result of Defendant's unauthorized actions.

10 381. Plaintiffs seek money damages and injunctive relief as provided under the statute.

11 **COUNT TWELVE**

12 **VIOLATION OF CALIFORNIA COMPUTER DATA ACCESS AND FRAUD ACT**
13 **Cal. Penal Code § 502**

14 382. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

15 383. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without
16 permission accessing, taking and using Plaintiffs' and the Class Members' personally identifiable
17 information.

18 384. Defendant accessed, copied, used, made use of, interfered with, and/or altered data
19 belonging to Plaintiffs and Class Members: (1) in and from the State of California; (2) in the states
20 in which the Plaintiffs and the Class Members are domiciled; and (3) in the states in which the
21 servers that provided services and communication links between Plaintiffs and the Class Members
22 and Google.com and other websites with which they interacted were located.

23 385. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal
24 action under this section, a person who causes, by any means, the access of a computer, computer
25 system, or computer network in one jurisdiction from another jurisdiction is deemed to have
26 personally accessed the computer, computer system, or computer network in each jurisdiction."

27 386. Defendants have violated California Penal Code § 502(c)(1) by knowingly and
28 without permission altering, accessing, and making use of Plaintiffs and Class Members' personally

1 identifiable data in order to execute a scheme to defraud consumers by utilizing and profiting from
2 the sale of their personally identifiable data, thereby depriving them of the value of their personally
3 identifiable data.

4 387. Defendants have violated California Penal Code § 502(c)(6) by knowingly and
5 without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class
6 Members' computer systems and/or computer networks.

7 388. Defendants have violated California Penal Code § 502(c)(7) by knowingly and
8 without permission accessing, or causing to be accessed, Plaintiffs' and Class Members' computer
9 systems and/or computer networks.

10 389. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant" is
11 defined as "any set of computer instructions that are designed to ... record, or transmit information
12 within computer, computer system, or computer network without the intent or permission of the
13 owner of the information."

14 390. Defendants have violated California Penal Code § 502(b)(8) by knowingly and
15 without permission introducing a computer contaminant into the transactions between Plaintiffs
16 and the Class Members and websites; specifically, a "cookie" that intercepts and gathers
17 information concerning Plaintiffs' and the Class Members' interactions with certain websites,
18 which information is then transmitted back to Google.

19 391. As a direct and proximate result of Defendant's unlawful conduct within the
20 meaning of California Penal Code § 502, Defendant has caused loss to Plaintiffs and the Class
21 Members in an amount to be proven at trial. Plaintiffs and the Class Members are also entitled to
22 recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

23 392. Plaintiffs and the Class Members seek compensatory damages, in an amount to be
24 proven at trial, and declarative or other equitable relief.

25 393. Plaintiffs and the Class Members are entitled to punitive or exemplary damages
26 pursuant to Cal. Penal Code § 502(e)(4) because Defendant's violations were willful and, upon
27 information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil
28 Code § 3294.

COUNT THIRTEEN

**STATUTORY LARCENY
California Penal Code §§ 484 and 496**

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

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

395. Section 496(a) prohibits the obtaining of property “in any manner constituting theft.”

396. Section 484 defines theft, and provides:

Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

397. Section 484 thus defines “theft” to include obtaining property by false pretense.

398. Defendant intentionally designed a program that would operate in a manner unbeknownst to Plaintiffs whose computers were thus deceived into providing PI to Defendant.

399. Defendant acted in a manner constituting theft and/or false pretense.

400. Defendant stole, took, and/or fraudulently appropriated Plaintiffs’ PI without Plaintiffs’ consent.

401. Defendant concealed, aided in the concealing, sold, and/or utilized Plaintiffs’ PI that was obtained by Defendant for Defendant’s commercial purposes and the financial benefit of Defendant.

402. Defendant knew that Plaintiffs’ PI was stolen and/or obtained because Defendant designed the code that tracked Plaintiffs’ PI and operated it in a manner that was concealed and/or withheld from Plaintiffs.

403. The reasonable and fair market value of the unlawfully obtain personal data can be determined in the marketplace.

COUNT FOURTEEN

**VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW (“UCL”)
Cal. Bus. & Prof. Code § 17200, *et seq.***

1
2
3
4 404. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

5 405. The UCL prohibits any “unlawful, unfair, or fraudulent business act or practice and
6 unfair, deceptive, untrue, or misleading advertising.” Cal. Bus. & Prof. Code § 17200.

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

8 407. Google violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* (“UCL”) by engaging in
9 unlawful, unfair, and deceptive business acts and practices.

10 408. Google’s “unlawful” acts and practices include its violation of the Electronic
11 Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; the Stored Communications Act,
12 18 U.S.C §§ 2701, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;
13 the Computer Fraud and Abuse Act, 18 U.S. C.§ 1030(g); the California Computer Data Access
14 and Fraud Act, Cal. Penal Code § 502; California Statutory Larceny, Cal. Penal Code §§ 484 and
15 496; and the Common Law Right of Privacy.

16 409. Google’s conduct violated the spirit and letter of these laws, which protect property,
17 economic and privacy interests and prohibit unauthorized disclosure and collection of private
18 communications and personal information.

19 410. Google’s “unfair” acts and practices include its violation of property, economic and
20 privacy interests protected by the: Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et*
21 *seq.*; the Stored Communications Act, 18 U.S.C §§ 2701, *et seq.*; the California Invasion of Privacy
22 Act, Cal. Penal Code §§ 630, *et seq.*; the Computer Fraud and Abuse Act, 18 U.S. C.§ 1030(g); the
23 California Computer Data Access and Fraud Act, Cal. Penal Code § 502; California Statutory
24 Larceny, Cal. Penal Code §§ 484 and 496; and the Common Law Right of Privacy. To establish
25 liability under the unfair prong, Plaintiffs need not establish that these statutes were actually
26 violated, although the claims pleaded herein do so.

27 411. Google and Chrome promised Plaintiffs not to send their PI to Google even when
28 Plaintiffs were Un-Synched. Plaintiffs thus had no reason to know and could not have anticipated

1 this intrusion into their privacy by the disclosure to Google of Plaintiffs’ personal information.
2 Google’s conduct was immoral, unethical, oppressive, unscrupulous and substantially injurious to
3 Plaintiffs. Further, Google’s conduct narrowly benefitted its own business interests at the expense
4 of Plaintiffs’ fundamental privacy interests protected by the California Constitution and the
5 common law.

6 412. Google’s “fraudulent” acts or practices under the UCL include its
7 misrepresentations and omissions assuring Plaintiffs that their PI would not be sent to Google while
8 Un-Synched were intended to, were likely to, and did deceive reasonable consumers such as
9 Plaintiffs. Google also misrepresented its privacy practices by disguising third-party tracking
10 cookies as first-party tracking cookies, a practice already successfully challenged by the FTC in an
11 earlier unrelated action. *United States v. Google, Inc.*, 12-cv-4177-SI (N.D. Cal.). The information
12 that Google misrepresented and concealed would be, and is, material to reasonable consumers,
13 namely, that rather than not sharing the information at issue as represented, in fact that information
14 was shared with Google.

15 413. Plaintiffs have suffered injury-in-fact, including the loss of money and/or property
16 as a result of Google’s unfair, unlawful and/or deceptive practices, to wit, the unauthorized
17 disclosure and taking of their personal information which has value as demonstrated by its use and
18 sale by Google. Plaintiffs have suffered harm in the form of diminution of the value of their private
19 and personally identifiable data and content.

20 414. Google’s actions caused damage to and loss of Plaintiffs’ property right to control
21 the dissemination and use of their personal information and communications.

22 415. Google’s misrepresentations and omissions—all which emanated from California—
23 were material because they were likely to deceive reasonable consumers.

24 416. Google reaped unjust profits and revenues in violation of the UCL. This includes
25 Google’s profits and revenues from their targeted-advertising, improvements of Google’s other
26 products. Plaintiffs and the Class seek restitution and disgorgement of these unjust profits and
27 revenues.
28

1 417. Plaintiffs and class members seek all monetary and non-monetary relief allowed by
2 law, including restitution of all profits stemming from Google’s unfair, unlawful, and fraudulent
3 business practices; declaratory relief; reasonable attorneys’ fees and costs under California Code
4 of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

5 **COUNT FIFTEEN**

6 **PUNITIVE DAMAGES**
7 **Cal. Civ. Code § 3294**

8 418. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

9 419. Google has an obligation not to intercept Plaintiffs’ electronic communications
10 without first obtaining consent, and this obligation exists by law independent of any contract with
11 Plaintiffs.

12 420. California Civil Code Section 3294(a) allows Plaintiffs to recover additional
13 damages “for the sake of example and by way of punishing the defendant” if the defendant is guilty
14 of “oppression, fraud or malice.”

15 421. Google intentionally caused injury to Plaintiffs and other Un-Synched Chrome
16 Users by tracking their web use and collecting other PI without permission, and with a conscious
17 disregard for their rights, making Google guilty of “malice” as defined by Section 3294(c)(1).

18 422. Google also intentionally misrepresented the privacy settings of Chrome, which was
19 a material feature of the browser. Through Google’s misrepresentation and deceit, Google deprived
20 Plaintiffs and the other Un-Synched Chrome Users of property and privacy rights.

21 423. Google is liable for punitive damages in an amount to be determined at trial.

22 **COUNT SIXTEEN**

23 **DECLARATORY RELIEF**
24 **28 U.S.C. § 2201(a)**

25 424. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

26 425. An actual and justiciable controversy within the jurisdiction of this Court exists
27 between the Plaintiffs and Google.
28

1 426. Plaintiffs seek an order declaring the rights of the parties arising out of the facts of
2 this case, specifically an order declaring:

- 3 a. The Chrome Privacy Notice is a part of the contract between Chrome users
4 and Google;
- 5 b. The data collected by Google from Chrome is Personal Information under the
6 terms of the contract and under California law;
- 7 c. Google is in breach of the its contracts with Plaintiffs and Signed-Out
8 Chrome Users by causing PI to be sent from Chrome to Google;
- 9 d. Google has violated the privacy rights of Plaintiffs and other Signed-Out
10 Chrome Users by causing Chrome to collect and report users' PI to Google;
- 11 e. Plaintiffs have suffered privacy harm; and
- 12 f. Plaintiffs have suffered economic harm.

13 **VIII. PRAYER FOR RELIEF**

14 WHEREFORE, Plaintiffs respectfully request that this Court:

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

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

20 C. Permanently restrain Defendant, and its officers, agents, servants, employees and
21 attorneys, from installing cookies on its users' computers that could track the users' computer usage
22 after logging out of Google or otherwise violating its policies with users;

23 D. Award Plaintiffs and the Class their reasonable costs and expenses incurred in this
24 action, including counsel fees and expert fees; and

25 E. Grant Plaintiffs such further relief as the Court deems appropriate.

26
27
28

1 **IX. JURY TRIAL DEMAND**

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

3 Dated: July 27, 2020

4 **BLEICHMAR FONTI & AULD LLP**

KAPLAN, FOX & KILSHEIMER LLP

5 By: /s/ Lesley Weaver

By: /s/ David A. Straite

6 Lesley Weaver (Cal. Bar No. 191305)
7 Angelica M. Ornelas (Cal. Bar No. 285929)
8 Joshua D. Samra (Cal. Bar No. 313050)
9 555 12th Street, Suite 1600
10 Oakland, CA 994607
11 Tel.: (415) 445-4003
12 Fax: (415) 445-4020
13 *lweaver@bfalaw.com*
14 *aornelas@bfalaw.com*
15 *jsamra@bfalaw.com*

David A. Straite (*pro hac vice* to be sought)
Aaron L. Schwartz (*pro hac vice* to be sought)
850 Third Avenue
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
dstraite@kaplanfox.com
aschwartz@kaplanfox.com

12 **SIMMONS HANLY CONROY LLC**

Laurence D. King (State Bar No. 206423)
Mario Choi (State Bar No. 243409)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Tel.: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com
mchoi@kaplanfox.com

13 By: /s/ Jay Barnes

14 Mitchell M. Breit (*pro hac vice* to be sought)
15 Jason ‘Jay’ Barnes (*pro hac vice* to be sought)
16 An Truong (*pro hac vice* to be sought)
17 Eric Johnson (*pro hac vice* to be sought)
18 112 Madison Avenue, 7th Floor
19 New York, NY 10016
20 Tel.: (212) 784-6400
21 Fax: (212) 213-5949
22 *mbreit@simmonsfirm.com*
23 *jaybarnes@simmonsfirm.com*

24 *Attorneys for Plaintiffs*

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)

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

I, Lesley E. Weaver, attest that concurrence in the filing of this document has been obtained from the other signatories. I declare under penalty of perjury that the foregoing is true and correct.

Executed this 27th day of July, 2020, at Oakland, California.

/s/ Lesley Weaver

Lesley E. Weaver

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Patrick Calhoun, Elaine Crespo, Hadiyah Jackson, and Claudia Kindler, on behalf of themselves and all others similarly situated,

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

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

Bleichmar Fonti & Auld LLP, 555 12th Street, Suite 1600, Oakland, CA 94601, 415.445.4003

DEFENDANTS

Google LLC

Santa Clara

THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

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

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

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and incorporation status.

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

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, OTHER, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): Federal Wiretap Act, 18 U.S.C. § 2511

Brief description of cause: Breach of contract and invasion of privacy

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$

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

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) SAN FRANCISCO/OAKLAND SAN JOSE EUREKA-MCKINLEYVILLE

DATE 07/27/2020

SIGNATURE OF ATTORNEY OF RECORD

/s/ Lesley E. Weaver

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

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

- I. a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
- c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
 - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
 - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
- (1) Original Proceedings. Cases originating in the United States district courts.
 - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
 - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
 - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”
- Date and Attorney Signature.** Date and sign the civil cover sheet.