

1 Mark C. Mao, CA Bar No. 236165  
2 Sean P. Rodriguez, CA Bar No. 262437  
3 Alexander J. Konik, CA Bar No. 299291  
4 **BOIES SCHILLER FLEXNER LLP**  
5 44 Montgomery St., 41<sup>st</sup> Floor  
6 San Francisco, CA 94104  
7 Tel.: (415) 293-6800  
8 Fax: (415) 293-6899  
9 [mmao@bsfllp.com](mailto:mmao@bsfllp.com)  
10 [srodriguez@bsfllp.com](mailto:srodriguez@bsfllp.com)  
11 [akonik@bsfllp.com](mailto:akonik@bsfllp.com)

12 James Lee (*pro hac* admission pending)  
13 Rossana Baeza (*pro hac* admission pending)  
14 **BOIES SCHILLER FLEXNER LLP**  
15 100 SE 2<sup>nd</sup> St., 28<sup>th</sup> Floor  
16 Miami, FL 33131  
17 Tel.: (305) 539-8400  
18 Fax: (303) 539-1307  
19 [jlee@bsfllp.com](mailto:jlee@bsfllp.com)  
20 [rbaeza@bsfllp.com](mailto:rbaeza@bsfllp.com)

21 *Attorneys for Plaintiffs*

22 **UNITED STATES DISTRICT COURT**  
23 **NORTHERN DISTRICT OF CALIFORNIA**

24 CHASOM BROWN, MARIA NGUYEN, and  
25 WILLIAM BYATT, individually and on  
26 behalf of all other similarly situated,

27 Plaintiffs,

28 v.

GOOGLE LLC and ALPHABET INC.,

Defendants.

Case No. 20-3664

**COMPLAINT**

**CLASS ACTION FOR**  
**(1) FEDERAL WIRETAP VIOLATIONS, 18**  
**U.S.C. §§ 2510, ET. SEQ.;**  
**(2) INVASION OF PRIVACY ACT**  
**VIOLATIONS, CAL. PENAL §§ 631 &**  
**632;**  
**(3) INVASION OF PRIVACY; AND**  
**(4) INTRUSION UPON SECLUSION.**

**DEMAND FOR JURY TRIAL**

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

**CLASS ACTION COMPLAINT**

Plaintiffs Chasom Brown, Maria Nguyen, and William Byatt, individually and on behalf of all others similarly situated, file this class action against defendants Google LLC and its parent company, Alphabet Inc. (collectively, “Google” or “Defendants”), and in support state the following:

**I. INTRODUCTION**

1. Protecting data privacy is critical in our rapidly modernizing society. People everywhere are becoming more aware (and concerned) that their personal communications are being intercepted, collected, recorded, or exploited for gain by technology companies they have come to depend on.

2. Well aware of consumers’ legitimate and reasonable concerns over privacy, Google assured, and continues to assure, its consumers and users that they, and not Google, are “in control of what information [they] share with Google.” Google further represents that “across our services, you can adjust our privacy settings to control what we collect and how your information is used.” Nothing could be further from the truth.

3. As discussed in more detail below, Google tracks and collects consumer browsing history and other web activity data *no matter what* safeguards consumers undertake to protect their data privacy. Indeed, even when Google users launch a web browser with “private browsing mode” activated (as Google recommends to users wishing to browse the web privately), Google nevertheless tracks the users’ browsing data and other identifying information.

4. Google accomplishes its surreptitious tracking through means that include: Google Analytics, Google Ad Manager, and various other application and website plug-ins, such as Google applications on mobile devices and the “Google Sign-In button” for websites. When an internet user visits a webpage or opens an app that uses such services (over 70% of all online publishers use such a service), Google receives detailed, personal information such as the user’s IP address (which may provide geographic information), what the user is viewing, what the user last viewed, and details about the user’s hardware. Google takes the data regardless of whether the user actually clicks on a Google-supported advertisement—or even knows of its existence. This means that billions of times

1 a day, Google causes computers around the world to report the real-time internet communications of  
2 hundreds of millions of people to Google.

3 5. Google has anticipated that consumers are understandably concerned that Google is  
4 tracking their personal information and browsing history. To assuage them, Google promises  
5 consumers that they can “browse the web privately” and stay in “control of what information [users]  
6 share with Google.” To prevent information from being shared with Google, Google recommends  
7 that its consumers need only launch a browser such as Google Chrome, Safari, Microsoft Edge, or  
8 Firefox in “private browsing mode.” Both statements are untrue. When users undertake either—or  
9 both—of the aforementioned steps, Google continues to track, collect, and identify their browsing  
10 data in real time, in contravention of federal and state laws on wiretapping and in violation of  
11 consumers’ rights to privacy.

12 6. Google’s practices infringe upon users’ privacy; intentionally deceive consumers;  
13 give Google and its employees power to learn intimate details about individuals’ lives, interests,  
14 and internet usage; and make Google “one stop shopping” for any government, private, or criminal  
15 actor who wants to undermine individuals’ privacy, security, or freedom. Through its pervasive  
16 data tracking business, Google knows who your friends are, what your hobbies are, what you like  
17 to eat, what movies you watch, where and when you like to shop, what your favorite vacation  
18 destinations are, what your favorite color is, and even the most intimate and potentially  
19 embarrassing things you browse on the internet—regardless of whether you follow Google’s advice  
20 to keep your activities “private.” Indeed, notwithstanding consumers’ best efforts, Google has made  
21 itself an unaccountable trove of information so detailed and expansive that George Orwell could  
22 never have dreamed it.

23 7. Google must be held accountable for the harm it has caused to its users in order to  
24 ensure it cannot continue to engage in the covert and unauthorized data collection from virtually every  
25 American with a computer or phone. This action arises from Google’s unlawful and intentional  
26 interception and collection of individuals’ confidential communications without their consent, even  
27 when those individuals expressly follow Google’s recommendations to prevent the tracking or  
28 collection of their personal information and communications. Beyond the California Constitution,

1 federal and state privacy laws recognize individuals’ reasonable expectations of privacy in  
2 confidential communications under these circumstances. Federal privacy laws prohibit  
3 unauthorized interception, access, and use of the contents in electronic communications. California  
4 law similarly prohibits, among other things, eavesdropping, recording, and sharing of confidential  
5 communications without the consent of all parties to the communication.

6 8. Plaintiffs are Google subscribers whose internet use was tracked by Google between  
7 June 1, 2016 and the present (the “Class Period”), while browsing the internet from a browser in  
8 “private browsing mode.” They bring federal and California state law claims on behalf of other  
9 similarly-situated Google subscribers in the United States (the “Class”) arising from Google’s  
10 knowing and unauthorized interception and tracking of users’ internet communications and activity,  
11 and knowing and unauthorized invasion of consumer privacy.

12 **II. THE PARTIES**

13 9. Plaintiff Mr. Chasom Brown (“Brown”) is an adult domiciled in Los Angeles,  
14 California. Brown had an active Google account during the entire Class Period.

15 10. Plaintiff Ms. Maria Nguyen (“Nguyen”) is an adult domiciled in Los Angeles,  
16 California. Nguyen had an active Google account during the entire Class Period.

17 11. Plaintiff Mr. William Byatt (“Byatt”) is an adult domiciled in Florida. Byatt had an  
18 active Google account during the entire Class Period.

19 12. Defendant Google is a Delaware limited liability company with a principal place of  
20 business at what is officially known as The Googleplex, 1600 Amphitheatre Parkway, Mountain  
21 View, California 94043. Google regularly conducts business throughout California and in this  
22 judicial district. Google is one of the largest technology companies in the world and conducts product  
23 development, search, and advertising operations in this district.

24 ///

25 ///

26 ///

27 ///

28 ///



1 19. Intradistrict Assignment. A substantial part of the events and conduct which give  
2 rise to the claims herein occurred in Santa Clara County.

#### 3 IV. FACTUAL ALLEGATIONS

##### 4 A. Google's Persistent Tracking Through Its Analytics and Ad Manager 5 Products

6 20. Over 70% of online websites and publishers on the internet (altogether "Websites")  
7 utilize Google's website visitor-tracking product, "Google Analytics." Google Analytics is a  
8 "freemium" service Google makes available to Websites that provides data analytics and  
9 attribution about the origins of a Website's traffic, demographics, frequency, browsing habits on  
10 the Website, and other data about visitors.

11 21. Google Analytics is "free" to implement, but the associated data and attribution  
12 reports come at a price tag when Websites want more specific information. Websites can obtain  
13 free general reports with pseudo-anonymous data regarding visitors. To obtain more specific and  
14 granular data about visitors, Websites must pay a substantial fee, such as by paying for Google's  
15 DV360, Ad Hub, or Google Audience products.

16 22. To implement Google Analytics, Google asks that Websites embed Google's own  
17 custom code into their existing webpage code. When a consumer visits a Website, his or her  
18 browser communicates a request to the Website's servers to send the computer script to display  
19 the Website. This communication and request for content from the consumer is often referred to  
20 as a HTTP GET request, to which the Website's servers respond with the computer code script to  
21 display the contents of the Website. The consumer's browser then begins to read Google's custom  
22 code along with the Website's own code when loading the Website from the Website's server.  
23 Two sets of code are thus automatically run as part of the browser's attempt to load and read the  
24 Website pages—the Website's own code, and Google's embedded code.

25 23. Google designed its Analytics code such that when it is run, Google causes the  
26 user's browser to send his or her personal information to Google and its servers in California, such  
27 as the user's IP address, URL address and particular page of the Website that is being visited, and  
28 other information regarding the user's device and browser. This is almost always done without  
the user's knowledge, in response to the consumer's request for information from the Website's

1 server. Google does not require that Websites disclose upfront that Google is collecting the  
2 visitors' information regardless of what they do, and as further discussed below, Google does not  
3 tell its users which websites implement Google Analytics. There is no effective way for consumers  
4 to avoid Google Analytics.

5 24. This practice allows Google to intercept, track, and collect more communications  
6 that reveal personal and consumer data than any company in the world. Since more than 70% of  
7 Websites use Google Analytics, Google is able to track a staggering amount of personal and  
8 consumer data online in real time. With virtually every click of the mouse to initiate a consumer's  
9 request, Google intercepts a signal and sends it to its own servers. Those signals contain  
10 consumers' personal viewing information and requests, which Google collects, reads, analyzes the  
11 contents of, and organizes based on consumers' prior histories. Google then uses the personal  
12 information obtained through this routine practice of interception to advance its business interests.

13 25. In addition to Google Analytics, over 70% of online publishes utilize another  
14 Google tracking and advertising product, called "Google Ad Manager" (formerly known as  
15 "DoubleClick For Publishers" or "DFP").

16 26. Like Google Analytics, Google Ad Manager requires Google code to be embedded  
17 into the Website's code, which is also run automatically whenever a user's browser loads the  
18 Website, as part of the consumer's request for the contents of the Website from the Website  
19 servers. The code essentially tells the browser what Google advertisements to display along with  
20 the Website's actual content, so that ads are served on behalf of Google's advertising customers.

21 27. In addition to serving ads, however, the Ad Manager code also causes users'  
22 browsers to send their personal information to Google and its servers in California, allowing  
23 Google to track visitors and traffic in much the same way as Google Analytics. To display a  
24 webpage with an ad served by Ad Manager, Google's code again extracts the visitor's IP address,  
25 browser and device information, the URL page, and content the visitor's device is displaying in  
26 real time. This occurs every time a user opens a Website containing the Google Ad Manager code.  
27 As with Google Analytics, Google does not require that Websites disclose upfront that Google is  
28 collecting the visitors' information regardless of what they do, and as further discussed below,

1 Google does not tell its users which websites implement Google Ad Manager. There is no effective  
2 way for consumers to avoid Google Ad Manager.

3 28. Thus, unbeknown to most consumers, Google constantly tracks what they request  
4 and read, click by click and page by page, in real time.<sup>2</sup>

5 **B. Google’s Misrepresentations About Data Privacy**

6 29. Over the last few years, the public, legislators, and courts have become increasingly  
7 aware of online threats to consumer privacy—including threats posed by powerful technology  
8 companies that have become household names. Google has responded by giving users the false  
9 impression that they can prevent Google from tracking their browsing history and collecting their  
10 personal data online. In Google’s Privacy Policy, Google makes numerous assurances about how  
11 users can “control” the information users share with Google, and that they can surf the web  
12 anonymously and without their communications with websites being intercepted.

13 30. Google’s Privacy Policy explicitly states that “you can adjust your privacy settings  
14 to control what we collect and how your information is used.”

15 on Google or watching YouTube videos. You can also choose to browse the web  
16 privately using Chrome in Incognito mode. And across our services, you can adjust  
17 your privacy settings to control what we collect and how your information is used.

18 31. On the “Go to My Activity” page of the Privacy Policy, Google reiterates that  
19 “My Activity allows you to review and *control data that’s created when you use Google*  
20 *services*, like searches you’ve done.”

---

21  
22  
23  
24 <sup>2</sup> The technical explanation is that when an individual internet user visits a web page, his or her  
25 browser sends a message called a “GET request” to the web page’s server. The GET request serves  
26 two purposes: it first tells the website what information is being requested and then instructs the  
27 website to send the information back to the user. The GET request also transmits a referer header  
28 containing the personally-identifiable URL information. Typically, this communication occurs  
only between the user’s web browser and the third-party website. On websites with Google code  
such as Google Analytics and Ad Manager, however, Google’s code directs the user’s browser to  
copy the referer header from the GET request and then send a separate but identical GET request  
and its associated referer header to Google’s server. It is through this duplication and collection  
of GET requests that Google compiles users’ browsing histories.



## Ways to review & update your information



### My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

[Go to My Activity](#)

32. When users click on “Go to My Activity” to control their data, they are presented with the option to “Learn more.” When users click on “Learn more,” they are taken to a page where they are supposed to be able to “View & control activity in your account.” On that page, Google states that you may “[s]top saving activity temporarily. . . . You can search and browse the web privately,” embedding a hyperlink to the “Search & Browse Privately” page. *See* SEARCH & BROWSE PRIVATELY, [https://support.google.com/websearch/answer/4540094?hl=en&ref\\_topic=3036132](https://support.google.com/websearch/answer/4540094?hl=en&ref_topic=3036132) (last visited May 29, 2020).

33. On the “Search & Browse Privately” page, Google once again reiterates that the user, not Google, is “in control of what information [a user] . . . share[s] with Google . . . .” Google states simply that consumers enabling “private browsing mode” on their browsers will allow consumers to “browse the web privately”:

#### **Search & browse privately**

You're in control of what information you share with Google when you search. **To browse the web privately**, you can use private browsing, sign out of your account, change your custom results settings, or delete past activity.

If you want to search the web without saving your search activity to your account, you can use private browsing mode in a browser (like Chrome or Safari).

#### **How private browsing works**

Private browsing works differently depending on which browser you use. Browsing in private usually means:

- The searches you do or sites you visit won't be saved to your device or browsing history.
- Files you download or bookmarks you create might be kept on your device.

- Cookies are deleted after you close your private browsing window or tab.
- You might see search results and suggestions based on your location or other searches you've done during your current browsing session.

**Important:** If you sign in to your Google Account to use a web service like Gmail, your searches and browsing activity might be saved to your account.

There is nothing on this page about Google Analytics or Google Ad Manager, or where and which websites online implement such data collection tools.

34. From the “View & control activity in your account” page referenced above, a consumer can also click the link, “See & control your Web & App Activity” on the right-hand side. See SEE & CONTROL YOUR WEB & APP ACTIVITY, [https://support.google.com/websearch/answer/54068?visit\\_id=6372555086257257422105376128&hl=en&rd=1](https://support.google.com/websearch/answer/54068?visit_id=6372555086257257422105376128&hl=en&rd=1) (last visited May 29, 2020). On that page, Google again represents that searching and browsing in “private browsing mode” will “turn off” any “search customization” “using search-related activity”:

**How Web & App Activity works when you’re signed out**

Your search and ad results may be customized using search-related activity even if you're signed out. To turn off this kind of search customization, you can search and browse privately. [Learn how.](#)

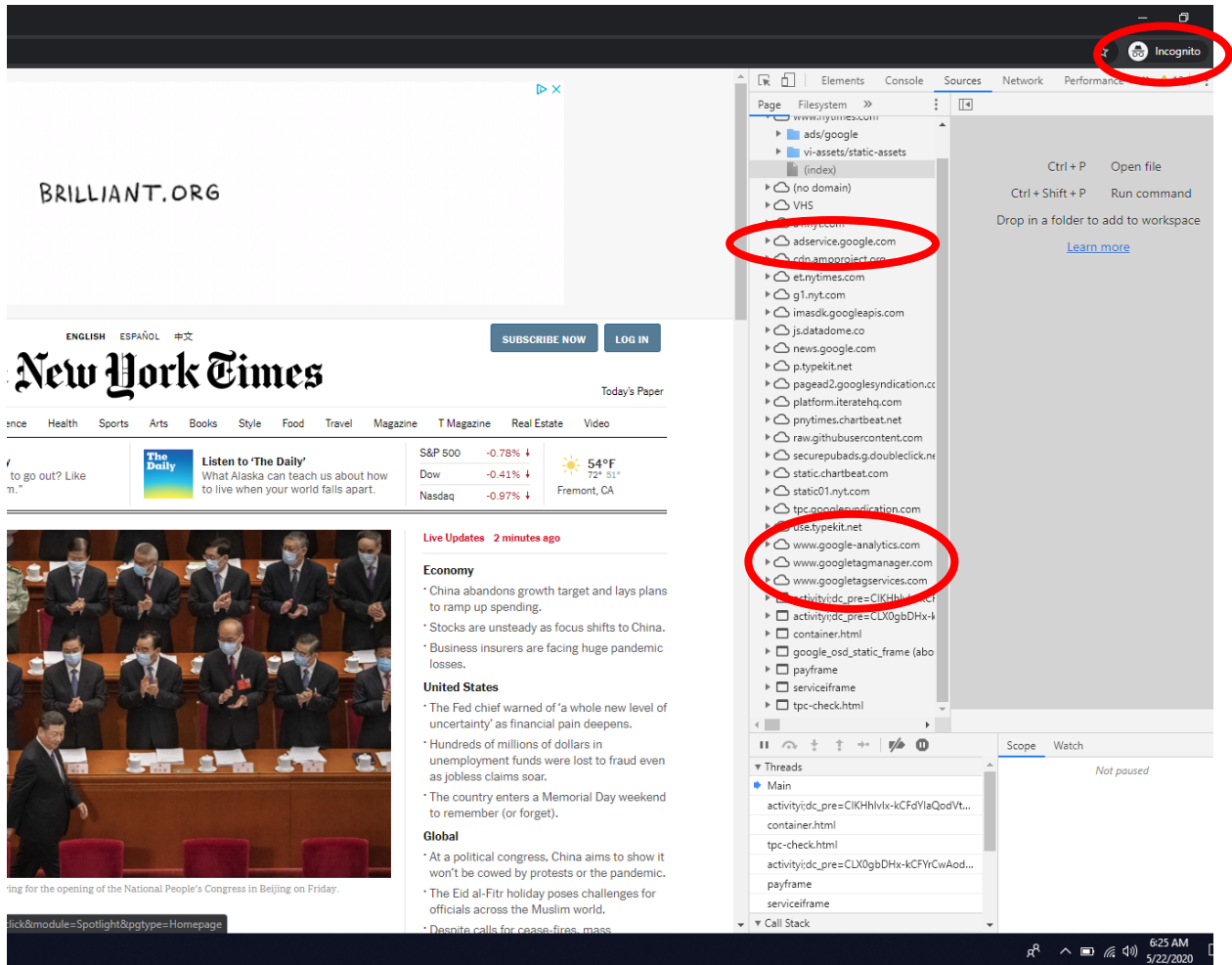
35. When users click the “Learn how” link, they are again redirected back to the “Search & Browse Privately” page. In other words, with Google repeatedly touting that users can “control” the information they share with Google, and with Google constantly referring back to its recommendations on how users may “browse the web privately,” the only reasonable impression that users are left with is the following: if they are searching or browsing the web in “private browsing mode,” Google will honor their request to be left alone and in private without further tracking.

36. As further explained herein, Google’s representations about how it does not track users under these conditions are completely false. Not only do consumers not know about what Google is doing to collect data on them, they have no meaningful way of avoiding Google’s data collection practices, even if they are following Google’s instructions to “browse the web privately.”

C. **Google Refuses to Turn Off Its Tracking of Users When They Are Browsing in “Private Browsing Mode”**

37. Despite its representations that users are in control of what information Google will track and collect, Google’s various tracking tools, including Google Analytics and Google Ad Manager, are actually designed to automatically track users when they visit webpages—*no matter what settings a user chooses*. This is true even when a user browses in “private browsing mode.”

38. Take, for example, someone who visits *The New York Times* website in private mode with his Google Chrome browser. Indeed, even when he is browsing with “private browsing mode” enabled, Google Analytics and Google Ad Manager continue to track his data, as demonstrated by the following screenshot:



39. Plaintiffs are informed and believe that even when users are browsing the internet in “private browsing mode,” Google continues to track them when they visit a Website that uses Google Analytics or Google Ad Manager. Google does so by collecting, at minimum, the

1 consumer's IP address, browser and device information, and the webpage content that the  
2 consumer is actually looking at. This is precisely the type of private, personal information users  
3 wish and expect to protect when they have taken these steps to control what information is shared  
4 with Google. Google's tracking occurred and continues to occur no matter how sensitive or  
5 personal users' online activities are. By tracking, collecting, and intercepting Plaintiffs' personal  
6 communications indiscriminately—regardless of whether Plaintiffs have attempted to avoid such  
7 tracking pursuant to Google's instructions—Google has gained a complete, cradle-to-grave profile  
8 of Plaintiffs without their consent.

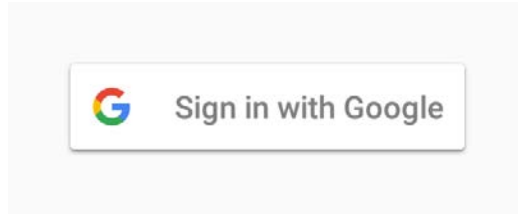
9 40. Google's justifications for doing so are baseless. Plaintiffs are informed and  
10 believe that Google has contended in private industry conversations, and in internal meetings and  
11 documents, that such surreptitious data collection is permissible, as it "aggregates the data" after  
12 the data has already been intercepted, collected, reviewed, and analyzed by Google. This does not  
13 mean that Google does not utilize and/or monetize this data in any way. Google does. It merely  
14 changes the form of storage after the data has served Google's nefarious uses. In any event, what  
15 Google says it does with users' communications with Websites after it has intercepted, analyzed,  
16 and used them for certain of its business purposes is cold comfort for those whose privacy it has  
17 already violated, because Google has repeatedly promised not to intercept or collect such  
18 communications in the first place. By doing so, it has already breached its users' expectations of  
19 privacy (that Google itself had created).

20 41. Plaintiffs are informed and believe that Google has also claimed in private industry  
21 conversations and in internal meetings and documents that its data collection practices are  
22 acceptable and not impermissible interceptions of communications, because Google is "acting on  
23 behalf of the website(s)", as their vendor. But that is simply not true. Instead, Google tells the  
24 Website owners—and their other advertisement vendors, which are often Google competitors—  
25 that data Google collects "on behalf of the website" actually belongs to Google, and not the  
26 website.

1           **D.     Google Can Track on Websites Using Other Methods as Well**

2           42.     In addition to Google Analytics and Ad Manager, Google actively and  
3 automatically tracks users who visit Websites in other ways, despite its assurances to the contrary.

4           43.     Much like other social media giants, Google has a “single sign on” button (the  
5 “Google Button”) that it causes various Websites to encode onto their webpages:



10          44.     Like other social media buttons, the Google Button has numerous tracking  
11 functions embedded into its code, which include the same type of automatic data collection  
12 implemented by Google’s Analytics and Ad Manager products described above. When a visitor’s  
13 browser loads the Google Button on the screen, Google’s code is called from its servers, which  
14 helps Google track the consumer.

15          45.     Google also allows “approved third parties” (such as Comscore, a data broker  
16 registered with California’s CCPA data broker registry) to provide digital pixels (“Google  
17 Approved Pixels”) to be embedded within the Websites’ code. *See, e.g.*, USE TRACKING PIXELS,  
18 <https://support.google.com/news/publisher-center/answer/9603438?hl=en> (last visited May 29,  
19 2020). When the code for such pixels is run by user browsers, the pixels are displayed uniquely  
20 by each browser/device combination because of certain digital signatures unique to each browser  
21 and device. By tracking these pixels and the unique resulting displays, Google and its data-broker  
22 partners are able to track and “measure” consumers across the web.

23          46.     Like Google Analytics and Ad Manager, the Google Button and Google Approved  
24 Pixels help the tech giant track consumers across the web in real time, even when they are in  
25 private mode.

26          47.     Perhaps most troubling is Google’s ability to match its web tracking capabilities  
27 with its Android operating system data and various Google application data on mobile devices. In  
28

1 a 2018 white paper entitled “Google Data Collection,”<sup>3</sup> Professor Douglas C. Schmidt of  
2 Vanderbilt University concluded that Google’s Android operating system, and several of Google’s  
3 mobile applications, are constantly sending system and location data to Google’s servers.  
4 Specifically, Professor Schmidt wrote:

5 Both Android and Chrome send data to Google even in the absence  
6 of any user interaction. Our experiments show that a dormant,  
7 stationary Android phone (with Chrome active in the background)  
8 communicated location information to Google 340 times during a  
9 24-hour period, or at an average of 14 data communications per  
10 hour. In fact, location information constituted 35% of all the data  
11 samples sent to Google.

12 Indeed, now that Google has acquired Nest and merged Nest’s data with data obtained via Google  
13 Home, Professor Schmidt’s analysis regarding Google’s ability to identify and track who and  
14 where we are is even more persistent and pernicious.

15 48. Through its passive data collection practices employed by Android, Google  
16 applications (e.g., Chrome and Maps), Google Home, and other Google applications and services,  
17 Google constantly collects users’ system and geolocation data. Plaintiffs are informed and believe  
18 that such passive collection happens even when a consumer is in the web browser’s “private  
19 browsing mode.” Indeed, the Arizona Attorney General recently filed a complaint against Google  
20 alleging that it deceptively tracks users based on various sources of location data. *See* Complaint,  
21 *Arizona v. Google LLC*, Arizona Sup. Ct. Case No. 2020-006219 (May 27, 2020). As a result,  
22 regardless of whether a user follows Google’s instructions advising how to be online without being  
23 tracked by Google, Google still leverages these other services to intercept and collect identifying  
24 information about who and where individual consumers are. Google accomplishes this task,  
25 among potentially other ways, by analyzing users’ device and geolocation information that it  
26 obtains through users’ numerous and unavoidable contacts with Google, and reconciling that with  
27 users’ device and geolocation information that it deceptively collects while users are employing

---

28 <sup>3</sup> Douglas C. Schmidt, *Google Data Collection*, DIGITAL CONTENT NEXT 1 (Aug. 15, 2018),  
[https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-  
Paper.pdf](https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf).

1 all of the safeguards Google has promised allow private online activity. Combined with Google's  
2 use of Analytics and Ad Manager, Google's ability to associate a particular user's online activity  
3 with his identity in a way that violates its promises about the ability to conduct online business  
4 without Google's tracking is unquestionable.

5 49. Indeed, media outlets such as The Register recently exposed Google's practice of  
6 using a browser level unique persistent identifier (a "X-client-Data Header") for individuals using  
7 Chrome, even when users clear their browser cache. Google reportedly sends this persistent  
8 identifier whenever the Chrome browser is viewing a page with Google Analytics or Ad  
9 Manager—presumably even when the user is in private mode. See Thomas Claburn, *Is Chrome*  
10 *Really Secretly Stalking You Across Google Sites Using Per-Install ID Numbers? We Reveal the*  
11 *Truth*, THE REGISTER (Feb. 5, 2020), [https://www.theregister.co.uk/2020/02/05/google\\_chrome](https://www.theregister.co.uk/2020/02/05/google_chrome_id_numbers/)  
12 [\\_id\\_numbers/](https://www.theregister.co.uk/2020/02/05/google_chrome_id_numbers/). In short, if you are using Google's Chrome browser, Google's code in that browser  
13 sends information back to Google's servers identifying the specific, individual browser (associated  
14 with you) that is viewing any Webpage that has implemented Ad Manager, Google Analytics, the  
15 Google Button, Google Approved Pixels, etc.

16 **E. Google Tracks for Its Own Nefarious Purposes, and Not Those of the**  
17 **Consumer**

18 50. Google represents on its website that "Google was founded on the belief that  
19 everything we do should always respect the user."

20 51. What Google does not publicly represent, however, is how it uses the endless  
21 amounts of personal and consumer data it intercepts and collects for its own business purposes.  
22 The more data Google reads, learns, and collects about a user, the more valuable the user profile  
23 it creates by using that information for third-party advertisers—and therefore, to Google's  
24 advertising business.

25 52. In a *Wired* article regarding Google's privacy practices, Professor Douglas  
26 Schmidt, who has studied Google's user data collection and retention policies, stated: Google's  
27 "business model is to collect as much data about you as possible and cross-correlate it so they can  
28 try to link your online persona with your offline persona. This tracking is just absolutely essential

1 to their business. ‘Surveillance capitalism’ is a perfect phrase for it.”<sup>4</sup> By collecting increasing  
2 amounts of user data, Google is able to leverage such data to grow its third-party advertising  
3 business and profit.

4 53. Through its spokespersons and in public-facing statements, Google continuously  
5 tries to give users the false impression that Google is merely acting on behalf of websites as a  
6 vendor, or on behalf of users to help customize their browsing experience. However, Google does  
7 not just serve the interests of users or partner websites; it also serves itself by using the data to  
8 improve its advertising products to generate further revenue.

9 54. In an NBC News article regarding Google’s endless trove of user data, Professor  
10 David Yoffie of the Harvard Business School stated, “Google is walking a very fine line. Search,  
11 plus Android gives Google amazing insight into individual behavior. Google’s stated privacy  
12 policies seem adequate, but the question that I cannot answer is whether Google’s stated policy  
13 and actual behavior are one and the same.”<sup>5</sup>

14 55. Plaintiffs are informed and believe that one of the most telling facts is that  
15 although Google often argues that it is collecting data on Websites for the Websites, Google often  
16 demands significant upgrades (e.g., such as to Google’s DV360, a very expensive upgrade) in  
17 order for the Websites to see specific visitor information. Otherwise, what the Websites believe  
18 are its own visitors’ information is not available to the Websites except at a general level. That  
19 Google holds such detailed information regarding visitors hostage is proof that Google collects  
20 consumer information on Websites primarily for its own use.

21 56. Plaintiffs are informed and believe that Google also uses the data it collects to  
22 iterate on existing Google products and develop new Google products. This collection, usage, or  
23 monetization of user data contravenes the steps Plaintiffs and Class members have taken to try to  
24 control their information from being tracked or used by Google in any way.

---

25  
26 <sup>4</sup> Lily Hay Newman, *The Privacy Battle to Save Google from Itself*, WIRED (Nov. 1, 2018),  
<https://www.wired.com/story/google-privacy-data/>.

27 <sup>5</sup> Ben Popken, *Google Sells the Future, Powered by Your Personal Data*, NBC NEWS (May 10,  
28 2018), <https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501>.



V. **GOOGLE USERS REASONABLY EXPECT THAT THEIR PRIVATE COMMUNICATIONS WILL NOT BE INTERCEPTED, COLLECTED, OR MISUSED**

1  
2  
3 57. Plaintiffs and Class members had a reasonable expectation of privacy that when  
4 using a browser while in “private browsing mode,” Google would not intercept, collect, record,  
5 disclose, or otherwise misuse their personal communications.

6 58. Plaintiffs’ and Class members’ expectation of privacy is deeply enshrined in  
7 California’s Constitution. Article I, section 1 of the California Constitution provides: “All people  
8 are by nature free and independent and have inalienable rights. Among these are enjoying and  
9 defending life and liberty, acquiring, possessing, and protecting property, and pursuing and  
10 obtaining safety, happiness, *and privacy*.” The phrase “*and privacy*” was added by the “Privacy  
11 Initiative” adopted by California voters in 1972.

12 59. The phrase “and privacy” was added in 1972 after voters approved a proposed  
13 legislative constitutional amendment designated as Proposition 11. Critically, the argument in  
14 favor of Proposition 11 reveals that the legislative intent was to curb businesses’ control over the  
15 unauthorized collection and use of consumers’ personal information, stating:

16 The right of privacy is the right to be left alone...It prevents  
17 government and business interests from collecting and stockpiling  
18 unnecessary information about us and from misusing information  
19 gathered for one purpose in order to serve other purposes or to  
20 embarrass us. Fundamental to our privacy is the ability to control  
circulation of personal information. This is essential to social  
relationships and personal freedom.<sup>6</sup>

21 60. Consistent with the language and intent of Proposition 11, a number of studies  
22 examining the collection of consumers’ personal data confirms that the surreptitious taking of  
23 personal, confidential, and private information—as Google has done—violates expectations of  
24 privacy that have been established as general social norms. Privacy polls and studies uniformly  
25 show that the overwhelming majority of Americans consider one of the most important privacy  
26

27  
28 <sup>6</sup> BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS,  
GEN. ELECTION \*26 (Nov. 7, 1972).

1 rights to be the need for an individual’s affirmative consent before a company collects and shares  
2 a subscriber’s personal data. Indeed, a recent study by Consumer Reports shows that 92% of  
3 Americans believe that internet companies and websites should be required to obtain consent  
4 before selling or sharing their data and the same percent believe internet companies and websites  
5 should be required to provide consumers with a complete list of the data that has been collected  
6 about them.<sup>7</sup>

7 61. Similarly, a study published in the *Harvard Business Review*, shows that  
8 consumers are largely unaware of how their personal information is used by businesses, with less  
9 than 25% of consumers realizing that they share their communication history, IP addresses, and  
10 web-surfing history when using a standard web browser.<sup>8</sup> It is also simply common sense that  
11 Google should not intercept or collect user communications when users are browsing in “private  
12 browsing mode,” as these steps demonstrate a clear expectation that communications under these  
13 circumstances are intended to be private or confidential.

14 62. In addition, Google affirmatively represented to Plaintiffs and the Class that  
15 browsing the internet using a browser with “private browsing mode” activated, would allow them  
16 to be prevent Google from tracking their personal information, browsing history, or other web  
17 activity data. Specifically, Google made the following misrepresentations to mislead Plaintiffs  
18 and the Class into believing that taking such measures would prevent Google from tracking  
19 personal information:

- 20 • “***You’re in control*** of what information you share with Google when you search.”
- 21 • “You can use our services in a variety of ways to manage your privacy . . . across  
22 our services, ***you can adjust our privacy settings to control what we collect and***  
23 ***how your information is used.***”

---

24  
25 <sup>7</sup> *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*,  
26 CONSUMER REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

27 <sup>8</sup> Timothy Morey, Theodore Forbath & Allison Shoop, *Customer Data: Designing for*  
28 *Transparency and Trust*, HARV. BUS. REV. (May 2015), <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>.

- 1 • “Your search and ad results may be customized using search-related activity even  
2 if you’re signed out. *To turn off this kind of search customization, you can search  
3 and browse privately.*”
- 4 • “To browse the web privately, *you can use private browsing*, sign out of your  
5 account, change your custom results settings, or delete past activity.”

6 Importantly, Google did not represent in any disclosure to Plaintiffs or the Class that it would  
7 continue to intercept, track, and collect communications even when they used a browser while in  
8 “private browsing mode.”

## 9 VI. VALUE OF INTERCEPTED COMMUNICATIONS

10 63. Google’s continuous tracking of users is no accident. Google is one of the largest  
11 technology companies in the world. Google LLC and its parent Alphabet Inc. have over 1.5 billion  
12 active account users, and Alphabet Inc. boasts a net worth exceeding \$950 billion.

13 64. Google’s enormous financial success results from its unparalleled tracking and  
14 collection of consumer personal information and selling and brokering of that information to  
15 optimize advertisement services.

16 65. Over the last five years, virtually all of Google’s revenue was attributable to third  
17 party advertising, and it is continuously driven to find new and creative ways to leverage its access  
18 to users’ data in order to sustain its phenomenal growth.

19 66. Google profits from users by acquiring their sensitive and valuable personal  
20 information, which includes far more than mere demographic information and volunteered personal  
21 information like name, birth date, gender and email address. More importantly, when consumers  
22 use Google, it plants numerous tracking mechanisms on users’ computers and web-browsers, which  
23 allow Google to track users’ browsing histories and correlate them with user, device, and browser  
24 IDs.

25 67. The information Google tracks has and had massive economic value during the  
26 Class Period. This value is well understood in the e-commerce industry, and personal information  
27 is now viewed as a form of currency.

28 68. Professor Paul M. Schwartz noted in the *Harvard Law Review*:

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

7 Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–  
8 57 (2004).

9 69. Likewise, in *The Wall Street Journal*, former fellow at the Open Society  
10 Institute (and current principal technologist at the ACLU) Christopher Soghoian noted:

11 The dirty secret of the Web is that the “free” content and services that  
12 consumers enjoy come with a hidden price: their own private data.  
13 Many of the major online advertising companies are not interested in  
14 the data that we knowingly and willingly share. Instead, these parasitic  
15 firms covertly track our web-browsing activities, search behavior and  
16 geolocation information. Once collected, this mountain of data is  
17 analyzed to build digital dossiers on millions of consumers, in some  
18 cases identifying us by name, gender, age as well as the medical  
19 conditions and political issues we have researched online.

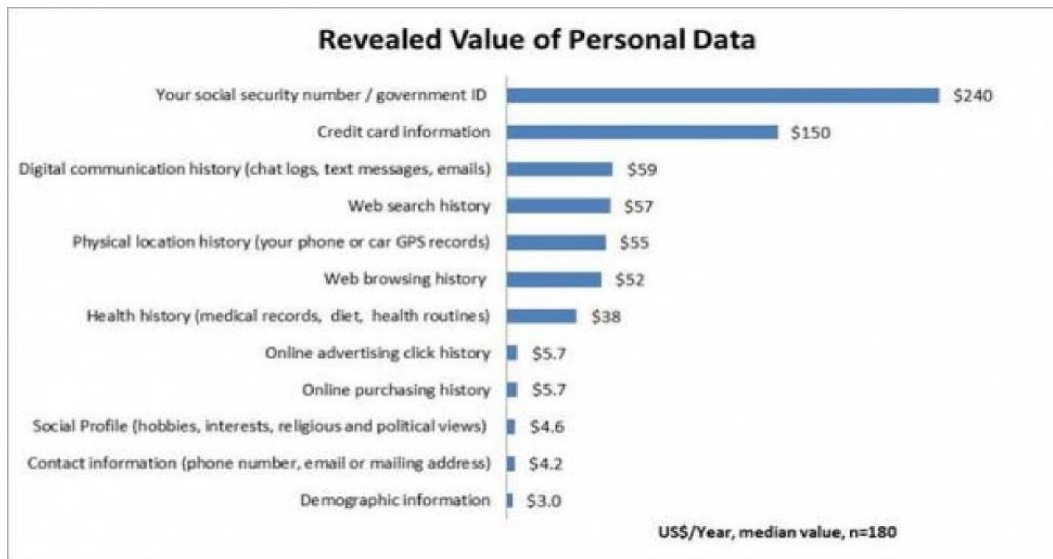
20 Although we now regularly trade our most private information for  
21 access to social-networking sites and free content, the terms of this  
22 exchange were never clearly communicated to consumers.

23 Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE  
24 WALL STREET JOURNAL (Nov. 15, 2011).

25 70. The cash value of users’ personal information provided during the Class Period  
26 to Google as a condition of membership can be quantified. For example, in a study authored  
27 by Tim Morey, researchers studied the value that 180 internet users placed on keeping personal  
28 data secure.<sup>9</sup> Contact information of the sort that Google requires was valued by the study  
participants at approximately \$4.20 per year. Demographic information was valued at  
approximately \$3.00 per year. But web browsing histories were valued at a much higher rate:  
\$52.00 per year. The chart below summarizes the findings:

---

<sup>9</sup> Tim Morey, *What’s Your Personal Data Worth?*, DESIGN MIND (Jan. 18, 2011),  
<https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html>.



71. Similarly, the value of user-correlated internet browsing history can be quantified, because Google itself was willing to pay users for the exact type of communications that Google illegally intercepted from Plaintiffs and other members of the Class during the Class Period. For example, Google Inc. had a panel during the Class Period (and still has one today) called “Google Screenwise Trends” which, according to the internet giant, is designed “to learn more about how everyday people use the Internet.”

72. Upon becoming a panelist, internet users would add a browser extension that shares with Google the sites they visit and how they use them. The panelists consented to Google tracking such information for three months in exchange for one of a number of “gifts,” including gift cards to retailers such as Barnes & Noble, Walmart, and Overstock.com.

73. After three months, Google also agreed to pay panelists additional gift cards “for staying with” the panel. These gift cards, mostly valued at exactly \$5, demonstrated conclusively that internet industry participants understood the enormous value in internet users’ browsing habits. Today, Google now pays Screenwise panelists up to \$3 *per week* to be tracked.

74. As demonstrated above, user-correlated URLs have monetary value. They also have non-monetary, privacy value. For example, in a recent study by the Pew Research Center, 93% of Americans said it was “important” for them to be “in control of who can get information” about them. Seventy-four percent said it was “very important.” Eighty-seven percent of

1 Americans said it was “important” for them not to have someone watch or listen to them without  
2 their permission. Sixty-seven percent said it was “very important.” And 90% of Americans said  
3 it was “important” that they be able to “control[] what information is collected about [them].”  
4 Sixty-five percent said it was very important.

5 75. Likewise, in a 2011 Harris Poll study, 76% of Americans agreed that “online  
6 companies, such as Google or Facebook, control too much of our personal information and know  
7 too much about our browsing habits.”

## 8 **VII. TOLLING OF THE STATUTE OF LIMITATIONS**

9 76. The applicable statutes of limitations have been tolled by Google’s knowing and  
10 active concealment and denial of the facts alleged herein.

11 77. Google has repeatedly represented that its users could prevent Google from  
12 tracking user information, such as by using a browser in “private browsing mode.” Indeed,  
13 nowhere did Google ever represent that it would continue to track user data once these steps were  
14 performed, nor has Google ever admitted that it will still attempt to collect, aggregate, and analyze  
15 user data so that it can continue to track individual users even when the user has followed Google’s  
16 instructions on how to browse privately.

17 78. Accordingly, Plaintiffs and the Class could not have reasonably discovered the  
18 truth about Google’s practices until shortly before this class litigation was commenced. They only  
19 learned of the truth in the weeks leading up to the filing of this Complaint.

## 20 **VIII. PLAINTIFF-SPECIFIC FACTUAL ALLEGATIONS**

21 79. Plaintiff Brown is an adult domiciled in California and has an active Google  
22 account and had an active account during the entire proposed Class Period.

23 80. He accessed the internet and sent and received communications with Websites on  
24 several computing devices that were not shared devices.

25 81. Since at least 2016, Mr. Brown has been a user of various Google products,  
26 including Google Maps, Waze, Gmail, and the Chrome browser. At various times since 2016,  
27 including between February 28 and May 31, 2020, Mr. Brown visited several major websites using  
28 Chrome, in incognito mode, on his Android devices, which included Android mobile phones and

1 laptops. These websites included but are not limited to Apartments.com, CNN.com, and *The LA*  
2 *Times*, and other private websites, and Google in in possession of a full record of these Websites.  
3 Although Mr. Brown did not know at that time, Plaintiffs are informed and believe now that  
4 Google was still tracking Mr. Brown, via various Android and Google-branded software and  
5 services, in addition to the X-client-Data Header.

6 82. Google thereby tracked Mr. Brown and intercepted his communications with  
7 Websites. Many of these requests were URL requests that revealed what he viewed and when.

8 83. Mr. Brown is aware that he is able to sell his own personal data, via other websites  
9 such as Latome (<https://www.lotame.com/how-to-monetize-your-data/>) and Killi  
10 (<https://killi.io/earn/>). Unlike these other websites that ask for Mr. Brown's permission to sell his  
11 data in exchange for consideration, Google never asked for his permission, and instead  
12 impermissibly intercepts his communications with Websites, and sell information gleaned from  
13 such communications. Google's practices irreparably damage Mr. Brown's privacy and his ability  
14 to control his own personal rights and data.

15 84. Plaintiff Nguyen is an adult domiciled in California and has an active Google  
16 account and had an active account during the entire proposed Class Period.

17 85. She accessed the internet and sent and received communications with Websites on  
18 several computing devices that were not shared devices.

19 86. Since at least 2016, Ms. Nguyen has been a user of various Google products,  
20 including Google Maps, Waze, Gmail, and the Chrome browser. At various times since 2016,  
21 including between February 28 and May 31, 2020, Ms. Nguyen visited several major websites  
22 using Chrome, in incognito mode, on her Apple devices, which included her iPhone and  
23 MacBook. She also visited several major websites using Safari, in private mode, on her Apple  
24 devices. These Websites included various major shopping sites and online publishers of fashion,  
25 and Google is in possession of a full record of these Websites. Although Ms. Nguyen did not  
26 know at that time, Plaintiffs are informed and believe now that Google was still tracking Ms.  
27 Nguyen, via various Google-branded software and services.

28 87. However, Google thereby tracked Ms. Nguyen and intercepted her

1 communications with Websites. Many of these requests were URL requests that revealed what  
2 she viewed and when.

3 88. Ms. Nguyen is aware that she is able to sell her own personal data, via other  
4 websites such as Latome (<https://www.lotame.com/how-to-monetize-your-data/>) and Killi  
5 (<https://killi.io/earn/>). Unlike these other websites that ask for Ms. Nguyen's permission to sell  
6 her data in exchange for consideration, Google never asked for her permission, and instead  
7 impermissibly intercepts her communications with Websites, and sell information gleaned from  
8 such communications. Google's practices irreparably damage Ms. Nguyen's privacy and her  
9 ability to control her own personal rights and data.

10 89. Plaintiff Byatt is an adult domiciled in Florida and has an active Google account  
11 and had an active account during the entire proposed Class Period.

12 90. He accessed the internet and sent and received communications with Websites on  
13 several computing devices that were not shared devices.

14 91. Since at least 2016, Mr. Byatt has been a user of various Google products, including  
15 Google Maps, Waze, Gmail, and the Chrome browser. At various times since 2016, including  
16 between February 28 and May 31, 2020, Mr. Byatt visited several major websites using Chrome,  
17 in incognito mode, on his Android and Apple devices, which included Android mobile phones.  
18 These Websites included, *The New York Times* ([nytimes.com](http://nytimes.com)) and *The Washington Post*  
19 ([Washingtonpost.com](http://Washingtonpost.com)), and other private websites, and Google is in possession of a full record of  
20 these Websites. Although Mr. Byatt did not know at that time, Plaintiffs are informed and believe  
21 now that Google was still tracking Mr. Byatt, via various Android and Google-branded software  
22 and services, in addition to the X-client-Data Header.

23 92. Google thereby tracked Mr. Byatt and intercepted his communications with  
24 Websites. Many of these requests were URL requests that revealed what he viewed and when.

25 93. Mr. Byatt is aware that he is able to sell his own personal data, via other websites  
26 such as Latome (<https://www.lotame.com/how-to-monetize-your-data/>) and Killi  
27 (<https://killi.io/earn/>). Unlike these other websites that ask for Mr. Byatt's permission to sell his  
28 data in exchange for consideration, Google never asked for his permission, and instead



1 impermissibly intercepts his communications with Websites, and sell information gleaned from  
2 such communications. Google’s practices irreparably damage Mr. Byatt’s privacy and his ability  
3 to control his own personal rights and data.

4 94. None of these Plaintiffs consented to the tracking and interception of their  
5 confidential communications made while browsing in “private browsing mode.”

6 **IX. CLASS ACTION ALLEGATIONS**

7 95. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil  
8 Procedure on behalf of the following Classes and Subclasses:

- 9
- 10 • Class 1 – All Android device owners who viewed a website page  
11 containing Google Analytics or Ad Manager using such a device,  
12 and who were (a) in “private browsing mode” on that device’s  
13 browser, and (b) did not log into their Google account on that  
14 device’s browser during that session, but whose communications,  
15 including identifying information and online browsing history,  
16 Defendant Google nevertheless intercepted, received, or collected  
17 from June 1, 2016 through the present (the “Class Period”).
  - 18 • Class 2 – All individuals with a Google account who accessed a  
19 website page containing Google Analytics or Ad Manager using  
20 any non-android device, and who were (a) in “private browsing  
21 mode” in that device’s browser, and (b) did not log into their  
22 Google account on that device’s web browser during that session,  
23 but whose communications, including identifying information and  
24 online browsing history, Defendant Google nevertheless  
25 intercepted, received, or collected from June 1, 2016 through the  
26 present (the “Class Period”).

27 96. Excluded from the Class are: (1) the Court (including any Judge or Magistrate  
28 presiding over this action and any members of their families); (2) Defendants, its subsidiaries,  
parents, predecessors, successors and assigns, including any entity in which any of them have a  
controlling interest and its officers, directors, employees, affiliates, legal representatives;  
(3) persons who properly execute and file a timely request for exclusion from the Class; (4)  
persons whose claims in this matter have been finally adjudicated on the merits or otherwise  
released; (5) Plaintiffs’ counsel, Class counsel and Defendants’ counsel; and (6) the legal  
representatives, successors, and assigns of any such excluded persons.

1           97.     **Ascertainability:** Membership of the Class is defined based on objective criteria  
2 and individual members will be identifiable from Defendants’ records, including from Google’s  
3 massive data storage, consumer accounts, and enterprise services. Based on information readily  
4 accessible to it, Google can identify members of the Class who own an Android device or have a  
5 non-Android device with an associated Google account, who were victims of Google’s  
6 impermissible interception, receipt, or tracking of communications as alleged herein.

7           98.     **Numerosity:** The Class likely consists of millions of individuals. Accordingly,  
8 members of the Class are so numerous that joinder of all members is impracticable. Class  
9 members can be identified from Defendants’ records, including from Google’s consumer accounts  
10 and enterprise services.

11           99.     **Predominant Common Questions:** Common questions of law and fact exist as to  
12 all members of the Class and predominate over any questions affecting solely individual members  
13 of the Class. Common questions for the Class include, but are not limited to, the following:

- 14           a.     Whether Google represented that the Class could control what  
15                 communications of user information, browsing history, and web activity data  
16                 were intercepted, received, or collected by Google;
- 17           b.     Whether Google gave the Class a reasonable expectation of privacy that their  
18                 communications of user information, browsing history, and web activity data  
19                 were not being intercepted, received, or collected by Google when the Class  
20                 was using a browser while in “private browsing mode”;
- 21           c.     Whether Google in fact intercepted, received, or collected communications of  
22                 user information, browsing history, and web activity from the Class when the  
23                 Class was using a browser while in “private browsing mode”;
- 24           d.     Whether Google’s practice of intercepting, receiving, or collecting  
25                 communications of user information, browsing history, and web activity  
26                 violated state and federal privacy laws;
- 27           e.     Whether Google’s practice of intercepting, receiving, or collecting  
28                 communications of user information, browsing history, and web activity

1 violated state and federal anti-wiretapping laws;

2 f. Whether Google’s practice of intercepting, receiving, or collecting  
3 communications of user information, browsing history, and web activity  
4 violated any other state and federal tort laws;

5 g. Whether Plaintiffs and the Class are entitled to declaratory and/or injunctive  
6 relief to enjoin the unlawful conduct alleged herein; and

7 h. Whether Plaintiffs and the Class have sustained damages as a result of  
8 Google’s conduct, and if so, what is the appropriate measure of damages or  
9 restitution.

10 100. **Typicality:** Plaintiffs’ claims are typical of the claims of other Class members, as  
11 all members of the Class were uniformly affected by Google’s wrongful conduct in violation of  
12 federal and state law as complained of herein.

13 101. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the members  
14 of the Class and have retained counsel that is competent and experienced in class action litigation,  
15 including nationwide class actions and privacy violations. Plaintiffs and their counsel have no  
16 interest that is in conflict with, or otherwise antagonistic to the interests of the other Class  
17 members. Plaintiffs and their counsel are committed to vigorously prosecuting this action on  
18 behalf of the members of the Class, and they have the resources to do so.

19 102. **Superiority:** A class action is superior to all other available methods for the fair and  
20 efficient adjudication of this controversy since joinder of all members is impracticable. This proposed  
21 class action presents fewer management difficulties than individual litigation, and provides the  
22 benefits of a single adjudication, economies of scale, and comprehensive supervision by a single, able  
23 court. Furthermore, as the damages individual Class members have suffered may be relatively small,  
24 the expense and burden of individual litigation make it impossible for members of the Class to  
25 individually redress the wrongs done to them. There will be no difficulty in management of this  
26 action as a class action.

27 103. **California Law Applies to the Entire Class:** California’s substantive laws apply to  
28 every member of the Class, regardless of where in the United States the Class member resides.

1 Defendants' own Terms of Service explicitly states "California law will govern all disputes arising  
2 out of or relating to these terms, service specific additional terms, or any related services, regardless  
3 of conflict of laws rules. These disputes will be resolved exclusively in the federal or state courts of  
4 Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those  
5 courts." By choosing California law for the resolution of disputes covered by its Terms of Service,  
6 Google concedes that it is appropriate for this Court to apply California law to the instant dispute.  
7 Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and  
8 the Class under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and  
9 Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S. Constitution. California has significant  
10 contact, or significant aggregation of contacts, to the claims asserted by the Plaintiffs and all Class  
11 members, thereby creating state interests that ensure that the choice of California state law is not  
12 arbitrary or unfair. Defendants' decision to reside in California and avail itself of California's laws,  
13 and to engage in the challenged conduct from and emanating out of California, renders the application  
14 of California law to the claims herein constitutionally permissible. The application of California laws  
15 to the Class is also appropriate under California's choice of law rules because California has  
16 significant contacts to the claims of Plaintiffs and the proposed Class, and California has a greatest  
17 interest in applying its laws here.

18 104. Plaintiffs reserve the right to revise the foregoing class allegations and definitions  
19 based on facts learned and legal developments following additional investigation, discovery, or  
20 otherwise.

## 21 X. COUNTS

### 22 COUNT I

#### 23 VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. § 2510, *ET. SEQ.*

24 105. Plaintiffs hereby incorporate paragraphs 1 to 104 as if fully stated herein.

25 106. The Federal Wiretap Act, as amended by the Electronic Communications Privacy  
26 Act of 1986, prohibits the intentional interception of the contents any wire, oral, or electronic  
27 communication through the use of a device. 18 U.S.C. § 2511.

28 107. The Wiretap Act protects both the sending and receipt of communications.

1           108. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire,  
2 oral or electronic communication is intercepted.

3           109. Google’s actions in intercepting and tracking user communications while they were  
4 browsing the internet using a browser while in “private browsing mode” was intentional. On  
5 information and belief, Google is aware that it is intercepting communications in these  
6 circumstances and has taken no remedial action.

7           110. Google’s interception of internet communications that the Plaintiffs were sending  
8 and receiving while browsing the internet using a browser while in “private browsing mode” was  
9 done contemporaneously with the Plaintiffs’ sending and receipt of those communications. In fact,  
10 Google received the communications before the communication between the Plaintiffs and the  
11 various websites were completed.

12           111. The communications intercepted by Google included “contents” of electronic  
13 communications made from the Plaintiffs to Websites other than Google in the form of detailed  
14 URL requests, webpage browsing histories, and search queries which Plaintiffs sent to those  
15 websites and for which Plaintiffs received communications in return from those websites.

16           112. The transmission of data between Plaintiffs and the websites on which Google  
17 tracked and intercepted their communications without authorization while they were in “private  
18 browsing mode” were “transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some]  
19 nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or  
20 photooptical system that affects interstate commerce[.]” and were therefore “electronic  
21 communications” within the meaning of 18 U.S.C. § 2510(12).

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

- 23           a. The computer codes and programs Google used to track the Plaintiffs’  
24           communications while they were in “private browsing mode”;
- 25           b. The Plaintiffs’ browsers and mobile applications;
- 26           c. The Plaintiffs’ computing and mobile devices;
- 27           d. Google’s web and ad servers;
- 28           e. The web and ad-servers of websites from which Google tracked and

1 intercepted the Plaintiffs’ communications while they were using a web  
2 browser in “private browsing mode”;

3 f. The computer codes and programs used by Google to effectuate its  
4 tracking and interception of the Plaintiffs’ communications while using a  
5 web browser while in “private browsing mode”; and

6 g. The plan Google carried out to effectuate its tracking and interception of  
7 the Plaintiffs’ communications while using a web browser while in “private  
8 browsing mode.”

9 114. Google was not an authorized party to the communication because the Plaintiffs were  
10 unaware of Google’s redirecting of the referer URLs and webpage browsing histories to Google  
11 itself, did not knowingly send any communication to Google, were browsing the internet using a  
12 browser while in “private browsing mode,” when Google intercepted the communications between  
13 the Plaintiffs and websites other than Google. Google could not manufacture its own status as a  
14 party to the Plaintiffs’ communications with others by surreptitiously redirecting or intercepting  
15 those communications.

16 115. As illustrated herein, “the” communications between the Plaintiffs and websites  
17 were simultaneous to, but *separate* from, the channel through which Google acquired the contents  
18 of those communications.

19 116. The Plaintiffs did not consent to Google’s continued gathering of the user’s  
20 communications after enabling “private browsing mode on their web browser,” and thus never  
21 consented to Google’s interception of their communications. Indeed, Google represented to  
22 Plaintiffs and the public that users could “control . . . what information [they] share with Google”  
23 and “browse the web privately” by browsing in “private browsing mode.” Moreover, the  
24 communications intercepted by Google were plainly confidential, which is evidenced by the fact  
25 that Plaintiffs enabled “private browsing mode” in a manner consistent with Google’s own  
26 recommendations to prevent sharing of information with Google prior to accessing or  
27 communicating with the referer URLs and webpage browsing histories.

28 117. After intercepting the communications, Google then used the contents of the

1 communications knowing or having reason to know that such information was obtained through  
2 the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

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

8 **COUNT II**

9 **VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (“CIPA”)**  
10 **CALIFORNIA PENAL CODE §§ 631 AND 632**

11 119. Plaintiffs hereby incorporate paragraphs 1 to 118 as if fully stated herein.

12 120. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to  
13 638. The Act begins with its statement of purpose:

14 The Legislature hereby declares that advances in science and  
15 technology have led to the development of new devices and  
16 techniques for the purpose of eavesdropping upon private  
17 communications and that the invasion of privacy resulting from the  
18 continual and increasing use of such devices and techniques has  
19 created a serious threat to the free exercise of personal liberties and  
20 cannot be tolerated in a free and civilized society.

21 Cal. Penal Code § 630.

22 121. California Penal Code § 631(a) provides, in pertinent part:

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

1 122. California Penal Code § 632(a) provides, in pertinent part:

2 A person who, intentionally and without the consent of all parties to a  
3 confidential communication, uses an electronic amplifying or  
4 recording device to eavesdrop upon or record the confidential  
5 communication, whether the communication is carried on among the  
6 parties in the presence of one another or by means of a telegraph,  
7 telephone, or other device, except a radio, shall be punished by a fine  
8 not exceeding two thousand five hundred dollars . . . .

9 123. Under either section of the CIPA, a defendant must show it had the consent of all  
10 parties to a communication.

11 124. Google has its principal place of business in California; designed, contrived and  
12 effectuated its scheme to track its users while they were browsing the internet from a browser  
13 while in “private browsing mode”; and has adopted California substantive law to govern its  
14 relationship with its users.

15 125. At all relevant times, Google’s tracking and interceptions of the Plaintiffs’  
16 internet communications while using a browser in “private browsing mode” was without  
17 authorization and consent from the Plaintiffs.

18 126. Google’s non-consensual tracking of the Plaintiffs’ internet communications  
19 who were on their web browser or using a browser in “private browsing mode” was designed  
20 to attempt to learn at least some meaning of the content in the URLs.

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

- 25 a. The computer codes and programs Google used to track the Plaintiffs’  
26 communications while they were in “private browsing mode”;
- 27 b. The Plaintiffs’ browsers and mobile applications;
- 28 c. The Plaintiffs’ computing and mobile devices;
- d. Google’s web and ad servers;
- e. The web and ad-servers of websites from which Google tracked and



1 intercepted the Plaintiffs’ communications while they were using a web  
2 browser in “private browsing mode”;

3 f. The computer codes and programs used by Google to effectuate its  
4 tracking and interception of the Plaintiffs’ communications while using a  
5 web browser in “private browsing mode”; and

6 g. The plan Google carried out to effectuate its tracking and interception of  
7 the Plaintiffs’ communications while using a browser in “private browsing  
8 mode.”

9 128. Plaintiffs and the Class members have suffered loss by reason of these violations,  
10 including, but not limited to, violation of their rights to privacy and loss of value in their  
11 personally-identifiable information.

12 129. Pursuant to California Penal Code § 637.2, Plaintiffs and the Class members have  
13 been injured by the violations of California Penal Code §§ 631 and 632, and each seek damages  
14 for the greater of \$5,000 or three times the amount of actual damages, as well as injunctive relief.

15 **COUNT III**

16 **INVASION OF PRIVACY**

17 130. Plaintiffs hereby incorporate paragraphs 1 and 129 as if fully stated herein.

18 131. The right to privacy in California’s constitution creates a right of action against  
19 private entities such as Google.

20 132. The principal purpose of this constitutional right was to protect against unnecessary  
21 information gathering, use, and dissemination by public and private entities, including Google.

22 133. To plead a California constitutional privacy claim, a plaintiff must show an  
23 invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable  
24 expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a  
25 serious invasion of privacy.

26 134. As described herein, Google has intruded upon the following legally protected  
27 privacy interests:  
28

- 1 a. The Federal Wiretap Act as alleged herein;
- 2 b. The California Wiretap Act as alleged herein;
- 3 c. A Fourth Amendment right to privacy contained on personal computing  
4 devices, including web-browsing history, as explained by the United States  
5 Supreme Court in the unanimous decision of *Riley v. California*;
- 6 d. The California Constitution, which guarantees Californians the right to  
7 privacy;
- 8 e. Google’s Privacy Policy and policies referenced therein, and other public  
9 promises it made not to track or intercept the Plaintiffs’ communications or  
10 access their computing devices and web-browsers while browsing in  
11 “private browsing mode.”

12 135. Plaintiffs had a reasonable expectation of privacy under the circumstances in that  
13 Plaintiffs could not reasonably expect Google would commit acts in violation of federal and state  
14 civil and criminal laws; and Google affirmatively promised users it would not track their  
15 communications or access their computing devices or web-browsers while they were using a web  
16 browser while in “private browsing mode.”

17 136. Google’s actions constituted a serious invasion of privacy in that it:

- 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;
- 22 c. Violated dozens of state criminal laws on wiretapping and invasion of  
23 privacy, including the California Invasion of Privacy Act;
- 24 d. Invaded the privacy rights of hundreds of millions of Americans without  
25 their consent; and
- 26 e. Constituted the unauthorized taking of valuable information from hundreds  
27 of millions of Americans through deceit;

28 137. Committing criminal acts against hundreds of millions of Americans constitutes an

1 egregious breach of social norms that is highly offensive.

2 138. The surreptitious and unauthorized tracking of the internet communications of  
3 millions of Americans, particularly where, as here, they have taken active (and recommended)  
4 measures to ensure their privacy, constitutes an egregious breach of social norms that is highly  
5 offensive.

6 139. Google’s intentional intrusion into Plaintiffs’ internet communications and their  
7 computing devices and web-browsers was highly offensive to a reasonable person in that Google  
8 violated federal and state criminal and civil laws designed to protect individual privacy and against  
9 theft.

10 140. The taking of personally-identifiable information from hundreds of millions of  
11 Americans through deceit is highly offensive behavior.

12 141. Secret monitoring of web private browsing is highly offensive behavior.

13 142. Wiretapping and surreptitious recording of communications is highly offensive  
14 behavior.

15 143. Google lacked a legitimate business interest in tracking users while browsing the  
16 internet on a browser while in “private browsing mode,” without their consent.

17 144. Plaintiffs and the Class members have been damaged by Google’s invasion  
18 of their privacy and are entitled to just compensation and injunctive relief.

19 **COUNT IV**

20 **INTRUSION UPON SECLUSION**

21 145. Plaintiffs hereby incorporate paragraphs 1 to 144 as if fully stated herein.

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

24 147. In carrying out its scheme to track and intercept Plaintiffs’ communications while  
25 they were using a browser while in “private browsing mode” in violation of its own privacy  
26 promises, Google intentionally intruded upon the Plaintiffs’ solitude or seclusion in that it  
27 effectively placed itself in the middle of conversations to which it was not an authorized party.

28 148. Google’s tracking and interception were not authorized by the Plaintiffs, the

1 websites with which they were communicating, or even the Plaintiffs’ web-browsers.

2 149. Google’s intentional intrusion into their internet communications and their  
3 computing devices and web-browsers was highly offensive to a reasonable person in that they  
4 violated federal and state criminal and civil laws designed to protect individual privacy and against  
5 theft.

6 150. The taking of personally-identifiable information from hundreds of millions of  
7 Americans through deceit is highly offensive behavior, particularly where, as here, Plaintiffs took  
8 active (and recommended) measures to ensure their privacy.

9 151. Secret monitoring of web private browsing is highly offensive behavior.

10 152. Wiretapping and surreptitious recording of communications is highly offensive  
11 behavior.

12 153. Public polling on internet tracking has consistently revealed that the overwhelming  
13 majority of Americans believe it is important or very important to be “in control of who can get  
14 information” about them; to not be tracked without their consent; and to be in “control[] of what  
15 information is collected about [them].” The desire to control one’s information is only heightened  
16 while a person is browsing the internet in “private browsing mode.”

17 154. Plaintiffs and the Class members have been damaged by Google’s invasion of  
18 their privacy and are entitled to reasonable compensation including but not limited to  
19 disgorgement of profits related to the unlawful internet tracking.

20 **PRAYER FOR RELIEF**

21 WHEREFORE, Plaintiffs respectfully request that this Court:

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

24 B. Award compensatory damages, including statutory damages where available, to  
25 Plaintiffs and the Class members against Defendants for all damages sustained as a result of  
26 Defendants’ wrongdoing, in an amount to be proven at trial, including interest thereon;

27 C. Ordering Defendants to disgorge revenues and profits wrongfully obtained;

28 D. Permanently restrain Defendants, and their officers, agents, servants, employees

1 and attorneys, from intercepting, tracking, or collecting communications after class members used  
2 a browser while in “private browsing mode,” or otherwise violating its policies with users;

3 E. Award Plaintiffs and the Class members their reasonable costs and expenses  
4 incurred in this action, including counsel fees and expert fees; and

5 F. Grant Plaintiffs and the Class members such further relief as the Court deems  
6 appropriate.

7 **XI. JURY TRIAL DEMAND**

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

9  
10 Dated: June 2, 2020

**BOIES SCHILLER FLEXNER LLP**

11 */s/ Mark C. Mao*

12 Mark C. Mao

13 *Attorneys for Plaintiffs*