

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., 41st Floor
6 San Francisco, CA 94104
7 Tel.: (415) 293-6800
8 Fax: (415) 293-6899
9 mmao@bsfllp.com
10 srodriguez@bsfllp.com
11 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 2nd St., 28th Floor
16 Miami, FL 33131
17 Tel.: (305) 539-8400
18 Fax: (303) 539-1307
19 jlee@bsfllp.com
20 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

CLASS ACTION COMPLAINT

1
2 Plaintiffs Chasom Brown, Maria Nguyen, and William Byatt, individually and on behalf of
3 all others similarly situated, file this class action against defendants Google LLC and its parent
4 company, Alphabet Inc. (collectively, “Google” or “Defendants”), and in support state the
5 following:

I. INTRODUCTION

6
7 1. Protecting data privacy is critical in our rapidly modernizing society. People
8 everywhere are becoming more aware (and concerned) that their personal communications are
9 being intercepted, collected, recorded, or exploited for gain by technology companies they have
10 come to depend on.

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

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

21 4. Google accomplishes its surreptitious tracking through means that include: Google
22 Analytics, Google Ad Manager, and various other application and website plug-ins, such as Google
23 applications on mobile devices and the “Google Sign-In button” for websites. When an internet user
24 visits a webpage or opens an app that uses such services (over 70% of all online publishers use such
25 a service), Google receives detailed, personal information such as the user’s IP address (which may
26 provide geographic information), what the user is viewing, what the user last viewed, and details
27 about the user’s hardware. Google takes the data regardless of whether the user actually clicks on a
28 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 ///

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.