

1 Mark C. Mao, CA Bar No. 236165
2 Beko Reblitz-Richardson, CA Bar
3 No. 238027
4 Alexander J. Konik, CA Bar No. 299291
5 **BOIES SCHILLER FLEXNER LLP**
6 44 Montgomery St., 41st Floor
7 San Francisco, CA 94104
8 Tel.: (415) 293-6800
9 Fax: (415) 293-6899
10 mmao@bsfllp.com
11 brichardson@bsfllp.com
12 akonik@bsfllp.com

Jesse Panuccio (*pro hac* admission pending)
BOIES SCHILLER FLEXNER LLP
1401 New York Ave, NW
Washington, DC 20005
Tel.: (202) 237-2727
Fax: (202) 237-6131
jpanuccio@bsfllp.com

8 James Lee (*pro hac* admission pending)
9 Rossana Baeza (*pro hac* admission pending)
10 **BOIES SCHILLER FLEXNER LLP**
11 100 SE 2nd St., 28th Floor
12 Miami, FL 33131
13 Tel.: (305) 539-8400
14 Fax: (303) 539-1307
15 jlee@bsfllp.com
16 rbaeza@bsfllp.com

13 *Attorneys for Plaintiffs*

15 **UNITED STATES DISTRICT COURT**
16 **NORTHERN DISTRICT OF CALIFORNIA**

18 ANIBAL RODRIGUEZ and JULIEANNA
19 MUNIZ individually and on behalf of all
20 other similarly situated,

20 Plaintiffs,

21 v.

22 GOOGLE LLC and ALPHABET INC.,

23 Defendants.

Case No. 3:20-cv-4688

COMPLAINT

CLASS ACTION FOR
(1) FEDERAL WIRETAP VIOLATIONS,
18 U.S.C. §§ 2510, ET. SEQ.;
(2) INVASION OF PRIVACY ACT
VIOLATIONS, CAL. PENAL CODE
§§ 631 & 632;
(3) INVASION OF PRIVACY;
(4) COMPREHENSIVE COMPUTER
DATA ACCESS AND FRAUD ACT,
CAL. PENAL CODE § 502.

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

This action arises from the unlawful and intentional interception and collection of individuals’ confidential communications and data without their knowledge or consent, even when those individuals expressly follow the recommendations of defendants Google LLC and its parent company Alphabet Inc. (collectively, “Google” or “Defendants”) to prevent the interception or collection of their browsing and other activity on their mobile apps. Plaintiffs Anibal Rodriguez and JulieAnna Muniz, individually and on behalf of all others similarly situated, file this class action against Google, and in support state the following:

I. INTRODUCTION

1. Google promises user control and privacy. In reality, Google is a voyeur extraordinaire. Google is always watching. Even when it promises to look away, Google is watching. Every click, every website, every app—our entire virtual lives. Intercepted. Tracked. Logged. Compiled. Packaged. Sold for profit.

2. This case is about Google’s illegal interception of consumers’ private activity on consumer mobile applications (“apps”)—a huge and growing treasure trove of data that Google amasses by the second to sustain profits in its ever-growing share of the market for consumer advertising.

3. Protecting data privacy is critical in our increasingly virtual and interconnected society. People everywhere are becoming more aware and more concerned, that large corporations are intercepting, collecting, recording and exploiting for profit their personal communications and private information.

4. Well aware of these justified and growing concerns over privacy, Google—one of the world’s largest technology companies—has assured and continues to assure its consumers and users that when it comes to mobile app activity, they and not Google, are “in control of what information [they] share with Google.” For example, Google’s global Privacy Policy states on the first page:

When you use our services, you’re trusting us with your information. We understand this is a big responsibility and work hard to protect your information and *put you in control*.

1 ...
2 Our services include: ... *products that are integrated into third-*
3 *party apps* and sites, like ads and embedded Google Maps.

4 ...
5 *[A]cross our services, you can adjust your privacy settings to*
6 *control what we collect* and how your information is used.

7 (emphasis added).

8 5. Google purports to offer consumers the option to “control” what app browsing and
9 activity data Google collects by adjusting their privacy settings to “turn Web & App Activity off . .
10 . at any time” before opening or browsing mobile apps. Google repeatedly assures its consumers
11 that they need only “[t]urn Web & App Activity on or off” to control what app activity Google can
12 and cannot see.

13 6. Google’s privacy promises and assurances are blatant lies.

14 7. Google in fact intercepts, tracks, collects and sells consumer mobile app browsing
15 history and activity data *regardless of what* safeguards or “privacy settings” consumers undertake
16 to protect their privacy. Even when consumers follow Google’s own instructions and turn off “Web
17 & App Activity” tracking on their “Privacy Controls,” Google nevertheless continues to intercept
18 consumers’ app usage and app browsing communications and personal information. Indeed, even
19 if consumers completely avoid using Google-branded apps and devices, Google still tracks and
20 compiles their communications by covertly integrating Google’s tracking software into the products
21 of other companies. Google’s illegal practices extend to hundreds of thousands of smartphone apps,
22 such as apps for The New York Times, Lyft, Alibaba, The Economist and others.

23 8. Google accomplishes this surreptitious and unlawful interception, tracking, and data
24 collection of users’ app activity through its Firebase SDK (software development kits). Firebase
25 SDK is a suite of software tools that purports to provide additional functionality to an app, especially
26 if it is to be released for Android. Third-party apps use Firebase SDK because its implementation
27 is a prerequisite before Google allows access to its other tools such as Google Analytics, use of
28 Google’s ad exchanges (such as AdMob, explained below), and marketing of those apps on the
29 Google Play Store. Developers often have no choice but to use Firebase SDK because of Google’s
30 demands and market power, including with analytics, advertisements, and the Android mobile

1 operating system. Once third-party app developers implement Firebase SDK, however, Firebase
2 SDK allows Google to automatically and systematically intercept, track, and collect their users' app
3 activity data—regardless of whether those users turn off “Web & App Activity” in their settings.

4 9. Google's practices infringe upon consumers' privacy; intentionally deceive
5 consumers; give Google and its employees power to learn intimate details about individuals' lives,
6 interests, and app usage; and make Google a potential target for “one-stop shopping” by any
7 government, private, or criminal actor who wants to undermine individuals' privacy, security, or
8 freedom. Through its pervasive and unlawful communication interceptions and massive data
9 tracking and collection business, Google knows every user's friends, hobbies, political leanings,
10 culinary preferences, cinematic tastes, shopping activity, preferred vacation destinations, romantic
11 involvements, and even the most intimate and potentially embarrassing aspects of the user's app
12 browsing histories and usage—regardless of whether the user accepts Google's illusory offer to
13 keep such activities “private.” Indeed, notwithstanding consumers' best efforts, Google has made
14 itself an unaccountable trove of information so detailed and expansive that George Orwell himself
15 could not have imagined it.

16 10. Google must be held accountable for the harm it has caused to its consumers. And it
17 must be prevented from continuing to engage in the covert and unauthorized data tracking and
18 collection from virtually every American with a mobile phone. Beyond the California Constitution,
19 federal and state privacy laws recognize individuals' reasonable expectations of privacy in
20 confidential communications under these circumstances. Federal and California privacy laws
21 prohibit unauthorized interception, access, and use of the contents in electronic communications.
22 The European courts have also recently found the practices at issue illegal. Likewise, American
23 regulators are beginning to recognize Google's abusive practices for what they are.

24 11. Plaintiffs are individuals whose mobile app usage was tracked by Google during the
25 period after Google first offered users the ability to turn off “Web & App Activity” tracking and the
26 present (the “Class Period”) with his or her “Web & App Activity” turned off. Google's tracking
27 and data collection included detailed browsing history data collected by Google, whereby Google
28 created and monetized user information without those users' consent. Plaintiffs bring federal and

1 California state law claims on behalf of other similarly-situated Google subscribers in the United
2 States (the “Class”) arising from Google’s knowing and unauthorized interception, copying, taking,
3 use, and tracking of consumers’ internet communications and activity, and its knowing and
4 unauthorized invasion of consumer privacy.

5 II. THE PARTIES

6 12. Plaintiff JulieAnna Muniz is an adult domiciled in El Cerrito, California. She had
7 an active Google account during the entire Class Period.

8 13. Plaintiff Anibal Rodriguez is an adult domiciled in Homestead, Florida. He had an
9 active Google account during the entire Class Period.

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

15 15. Defendant Alphabet Inc. is a Delaware corporation, organized and existing under
16 the laws of the State of Delaware, with its principal place of business at what is officially known as
17 The Googleplex, 1600 Amphitheatre Parkway, Mountain View, California 94043-1351. Alphabet
18 is the parent holding company of Google LLC. Alphabet owns all the equity interests in Google
19 LLC.¹

20 III. JURISDICTION AND VENUE

21 16. This Court has personal jurisdiction over Defendants because their principal place
22 of business is in California. Additionally, Defendants are subject to specific personal jurisdiction
23 in this State because a substantial part of the events and conduct giving rise to Plaintiffs’ and the
24 Class’ claims occurred in this State.

25
26 ¹ During the 2015 reorganization, certain of Google LLC’s business segments were spun off and
27 separated into independent entities under the ownership of Alphabet Inc. At various times during
28 the Class Period, certain of the business segments re-merged with Google LLC under one corporate
structure. Accordingly, Alphabet Inc. and Google LLC both have been named as defendants in
order to ensure all corporate entities who may be found liable for any portion of the alleged
wrongdoing are part of this lawsuit.

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.