LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol (SBN 194857)
Melissa Gardner (SBN 289096)
Ian Bensberg (*pro hac vice pending*)
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
(415) 956-1000

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Nicholas Diamand (*pro hac vice pending*)
ndiamand@lchb.com
Douglas Cuthbertson (*admitted pro hac vice*)
dcuthbertson@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: 212.355.9500
Facsimile: 212.355.9592

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

JONATHAN DIAZ and LEWIS BORNMANN, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 5:21-cv-03080-NC

AMENDED COMPLAINT

CLASS ACTION

DEMAND FOR JURY TRIAL

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

TABLE OF CONTENTS

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

I. INTRODUCTION

Defendant Google LLC ("Google") co-created the Google-Apple Exposure Notification System ("GAEN") to assist state and local authorities deploying apps for mobile devices that conduct COVID-19 "contact-tracing," and implements GAEN in Android smartphones via Google Play Services (GPS), an application package developed by Google. Google unequivocally assures that it completely safeguards the sensitive information necessarily involved with COVID-19 contact tracing, including that your identity, your health information, and other personal information would be inaccessible to others, including Google. However, Google's implementation of GAEN means that sensitive contact tracing data and personally identifying information is placed on a device's system logs, accessed by dozens or even hundreds of third parties, and collected and used by these third parties for their own purposes, including by Google itself. As a result, Google has exposed and transmitted GAEN participants' private personal and medical information associated with contact tracing, including notifications to Android device users of their potential exposure to COVID-19.

The GAEN contact tracing system uses signals called "rolling proximity identifiers" broadcast through the Bluetooth radio on mobile devices that other mobile devices can detect and record, thereby providing information about proximate encounters with nearby participants. Google's GPS records both this outgoing and incoming data on each device's system log, such that Android device users running Google's software unwittingly expose and transmit not only their information to numerous third parties, but also information from unsuspecting GAEN users on other devices (including non-Android devices, such as iPhones) who come within range of them.

The exposed information is personally identifiable. The contact tracing apps themselves generate ostensibly-secure personal device identifiers, which change periodically as they are broadcast to other devices, and should be traceable to the device user only with a "key" held by the public health authorities. But in storage, these identifiers are maintained alongside other device identifiers known as MAC addresses, and in at least some cases, alongside yet other personal identifiers including the IP address of the wireless network, telephone number, and the

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

App user's email address. When this stored data is written to mobile device system logs, it becomes available to third parties with access to the logs. They, alone or in concert, can use the MAC addresses and other identifiers to trace the log files back to individual identities, locations, and other identifying attributes, effectively creating an alternative "key" of their own. For those who have reported testing positive, it enables third parties, as well as Google itself, to link that diagnosis back to the particular patient, defeating the purported anonymity Google claims for its service.

In February 2021, Google was informed of the security flaw in its implementation of GAEN that caused the data breach alleged herein. To date, Google has failed to inform the public that GAEN participants' private personal and medical information has left their devices and been exposed to and collected by third parties, *as well as by Google itself,* who in the ordinary course of business access the system logs and collect and read the sensitive information contained therein.

Accordingly, Plaintiffs Jonathan Diaz and Lewis Bornmann, on behalf of themselves and all others similarly situated, bring this action pursuant to the California Confidentiality of Medical Information Act and their common law and constitutional privacy rights to obtain a mandatory public injunction requiring Google to remediate the security flaw in its implementation and maintenance of the GAEN system, and for, *inter alia*, damages and restitution.

II. PARTIES

1. Plaintiff Jonathan Diaz is a citizen and resident of Alameda County, California.

2. Plaintiff Lewis Bornmann is a citizen and resident of Solano County, California.

3. Defendant Google LLC ("Google") is a Delaware limited liability company based at 1600 Amphitheatre Way, Mountain View, California, whose sole member is XXVI Holdings Inc. XXVI Holdings Inc. is a corporation incorporated in Delaware with its principal office in California.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

III. JURISDICTION

4. Under 28 U.S.C. § 1332(d), the Court has subject matter jurisdiction of Plaintiffs' state law claims because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least one class member is a citizen of a state that is neither Delaware nor California.

IV. INTRADISTRICT ASSIGNMENT

5. Pursuant to Civil L.R. 3-2(c), assignment to the San Jose Division of this District is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in Santa Clara County. Google developed, markets, and deploys its products throughout the United States, including in Santa Clara County. Additionally, Google is headquartered in Mountain View, California, which is located within Santa Clara County.

V. GOOGLE'S CONDUCT

A. Background: The COVID-19 Pandemic

6. In December 2019, a new strain of coronavirus known as SARS-CoV-2 appeared in China.

7. SARS-CoV-2 causes a highly infectious disease known as COVID-19.

8. COVID-19 spread swiftly across the globe. The World Health Organization declared it a global health emergency on January 20, 2020.

9. One potentially effective tool used by public health authorities to control the spread of infectious diseases like COVID-19 is called contact tracing.

10. In general, contact tracing means identifying everyone who has come into contact with an infected person to notify them they may have been infected, observe them for signs of infection, and isolate and treat them if they are infected.

11. The contact tracing protocol issued for COVID-19 by the U.S. Centers for Disease Control and Prevention provides that such notifications should be issued to anyone who has been within 6 feet of an infected person for at least 15 minutes within the past 14 days.[1]

---

[1] Ctrs. for Disease Control & Prevention, *Contact Tracing for COVID-19* https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/contact-tracing.html (Feb. 25, 2021).

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

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.