

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP  
Michael W. Sobol (SBN 194857)  
Melissa Gardner (SBN 289096)  
Ian Bensberg (*pro hac vice pending*)  
275 Battery Street, 29<sup>th</sup> 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  
BORNMAN, 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**

# TABLE OF CONTENTS

	Page
I. INTRODUCTION .....	1
II. PARTIES .....	2
III. JURISDICTION.....	3
IV. INTRADISTRICT ASSIGNMENT.....	3
V. GOOGLE’S CONDUCT .....	3
A. Background: The COVID-19 Pandemic .....	3
B. Google’s Exposure Notification System.....	4
C. How GAEN Works .....	6
D. Google Represents to the World That GAEN-Driven Contact Tracing Is Anonymous .....	9
E. Google’s Implementation of GAEN Exposes COVID-19 Tracing Data via Google’s System Logs .....	12
F. Google Has Been Collecting COVID-19 Tracing Data Along with Other Personally Identifiable Information from Devices’ System Logs.....	18
G. The Exposed COVID-19 Tracing Data is Personally Identifiable.....	19
H. Millions of App Users Are Affected by the GAEN Security Breach .....	21
I. Google Refuses to Satisfactorily Address This Vulnerability .....	22
VI. THE NAMED PLAINTIFFS’ EXPERIENCES .....	23
A. Plaintiff Lewis Bornmann .....	23
B. Plaintiff Jonathan Diaz.....	24
VII. CLASS ACTION ALLEGATIONS .....	25
VIII. CLAIMS FOR RELIEF .....	27
FIRST CLAIM FOR RELIEF Invasion of Privacy: Public Disclosure of Private Facts .....	27
SECOND CLAIM FOR RELIEF Invasion of Privacy: Intrusion Upon Seclusion .....	29
THIRD CLAIM FOR RELIEF California Constitution, Article 1, § 1 .....	30
FOURTH CLAIM FOR RELIEF California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56 <i>et seq.</i> .....	31
IX. PRAYER FOR RELIEF.....	35
X. DEMAND FOR JURY TRIAL.....	36

1 **I. INTRODUCTION**

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

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

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

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

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

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

## 19 **II. PARTIES**

- 20 1. Plaintiff Jonathan Diaz is a citizen and resident of Alameda County, California.
  - 21 2. Plaintiff Lewis Bornmann is a citizen and resident of Solano County, California.
  - 22 3. Defendant Google LLC ("Google") is a Delaware limited liability company based  
23 at 1600 Amphitheatre Way, Mountain View, California, whose sole member is XXVI Holdings  
24 Inc. XXVI Holdings Inc. is a corporation incorporated in Delaware with its principal office in  
25 California.
- 26  
27  
28

### 1 **III. JURISDICTION**

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

### 5 **IV. INTRADISTRICT ASSIGNMENT**

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

### 11 **V. GOOGLE'S CONDUCT**

#### 12 **A. Background: The COVID-19 Pandemic**

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

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

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

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

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

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

---

26  
27 <sup>1</sup> Ctrs. for Disease Control & Prevention, *Contact Tracing for COVID-19*  
28 <https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/contact-tracing.html> (Feb. 25, 2021).

# 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.