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 (*pro hac vice pending*)
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-3080

COMPLAINT

CLASS ACTION

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

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 Mobile Services, a collection of Google apps and APIs ("GMS"). Google unequivocally assures that it completely safeguards the sensitive information necessarily involved with COVID-19 contact tracing. However, because Google's implementation of GAEN allows this sensitive contact tracing data to be placed on a device's system logs and provides dozens or even hundreds of third parties access to these system logs, Google has exposed 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 GMS records both this outgoing and incoming data on each device's system log, such that Android device users running Google's software unwittingly expose 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. 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 to trace the identifiers 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 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 participants in GAEN have had their private personal and medical information exposed to third parties, who in the ordinary course of business may access the system logs from time to time, or that Google itself may access these logs.

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 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.

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]

B. Google's Exposure Notification System

12. In 2020, Google and Apple Inc. developed a system for digital contact tracing using smartphones called the Google-Apple Exposure Notification System ("GAEN").

13. In May 2020, Google implemented GAEN and made it available to public health authorities worldwide.[2]

14. GAEN acts a framework or platform on which a public health authority can build a mobile contact tracing application ("Contact Tracing App" or "App") for use in its jurisdiction.[3]

---

[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).

[2] David Burke, *An Update on Exposure Notifications*, Google (July 31, 2020), https://blog.google/inside-google/company-announcements/update-exposure-notifications.

[3] Google, *Exposure Notifications*, https://www.google.com/covid19/exposurenotifications (last visited Apr. 27, 2021).

15. Google advertises its implementation of GAEN as "[u]sing technology to help public health authorities fight COVID-19."[4]

16. In the United States, public health authorities in Alabama, Arizona, California, Colorado, Connecticut, Delaware, the District of Columbia, Guam, Hawai'i, Louisiana, Maryland, Michigan, Minnesota, Nevada, New Jersey, New York, North Carolina, Oregon, Pennsylvania, Puerto Rico, South Carolina, North Dakota, Wyoming, Utah, Virginia, Washington, and Wisconsin have released Contact Tracing Apps that use GAEN.[5]

17. In the United States, more than 28 million people, residents of each jurisdiction above, have downloaded Contact Tracing Apps that use GAEN or activated exposure notifications on their mobile devices.[6]

18. California's Contact Tracing App is called CA Notify and was developed by the California Department of Technology.[7]

19. Users of Apple devices in California may activate the functionality of CA Notify on their phones without having to download the App.[8]

20. CA Notify has been downloaded to about 9.5 million mobile devices.[9]

21. CA Notify has been downloaded to about 8.5 million Apple devices.[10]

---

[4] *Id.*

[5] Mishaal Rahman, *Here Are the Countries Using Google and Apple's COVID-19 Contact Tracing API*, XDA (Feb. 25, 2021, 2:27 PM), https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries.

[6] Lindsey Van Ness, *For States' COVID-19 Contact Tracing Apps, Privacy Tops Utility*, Government Technology (Mar. 22, 2021), https://www.govtech.com/health/For-States-COVID-19-Contact-Tracing-Apps-Privacy-Tops-Utility.html.

[7] Cal., *California Can Stop the Spread*, https://canotify.ca.gov/ (last visited Apr. 27, 2021); Cal. Dep't of Technology, *CA Notify*, https://play.google.com/store/apps/details?id=gov.ca.covid19.exposurenotifications (Apr. 5, 2021).

[8] Jason Pohl & Dale Kasler, *Did You Get a COVID-19 Warning from California's Phone App? Why You Probably Didn't*, The Sacramento Bee, https://www.sacbee.com/news/coronavirus/article249875513.html (Mar. 15, 2021, 3:56 PM).

[9] *Id.*

[10] *Id.* ("about nine times as many people have enrolled in CA Notify on an iPhone").

22. CA Notify has been downloaded to about 1 million Android devices.[11]

C. How GAEN Works

23. Contact Tracing Apps that use GAEN work on both devices running Google's Android operating system and devices running Apple's iOS operating system.

24. On both operating systems, contact tracing that uses GAEN works as follows: First, a user activates contact tracing on their device. For Android users, this requires the download of an App offered by their state public health authority. Since fall 2020 it has been possible for users of Apple devices in participating jurisdictions to activate GAEN on their phones directly from the device settings, without having to download and install a freestanding Contact Tracing App.[12]

25. Second, as part of the activation process, GAEN generates a unique, random-seeming sequence of characters called a Temporary Exposure Key ("Key") for the user.[13]

26. A new Key is generated once every 24 hours after installation.[14]

27. Third, the App uses the Key to generate a "rolling proximity identifier key," which then generates a different, unique, random-seeming sequence of characters called a "rolling proximity identifier" (RPI).[15]

---

[11] *Id.*

[12] Russell Brandom, *Apple and Google Announce New Automatic App System to Track COVID Exposures*, The Verge (Sept. 1, 2020, 12:00 PM), https://www.theverge.com/2020/9/1/21410281/apple-google-coronavirus-exposure-notification-contact-tracing-app-system; Google, *Use the COVID-19 Exposure Notifications System on Your Android Phone*, https://support.google.com/android/answer/9888358 (last visited Apr. 27, 2021) ("To use the system, you need to download an official app from your region's government public health authority.").

[13] Apple & Google, *Exposure Notification: Cryptography Specification* 6 (Apr. 23, 2020), https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf [hereinafter *Cryptography Specification*].

[14] Apple & Google, *Exposure Notification: Bluetooth Specification* 3 (Apr. 23, 2020), https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf [hereinafter *Bluetooth Specification*].

[15] *Cryptography Specification*, *supra* note 13, at 6–7.

28. As the user goes about her day, her phone broadcasts the RPI over its Bluetooth radio to other users' phones within range, whose devices receive and record the broadcasted incoming RPI.[16]

29. The App generates a new RPI for the user's phone every 15 or 20 minutes.[17]

30. The App records all the RPIs it broadcasts.[18]

31. As the user goes about her day, her phone broadcasts the identifier known as a MAC address (typically, a unique string of characters meant to identify a device on a network) in the course of transmitting her RPIs over its Bluetooth radio to other users' phones within range, whose devices record the RPIs but also incidentally record the MAC address and associate the MAC address with the RPI.[19]

32. In general, because Bluetooth transmissions include the transmitting device's MAC address, Bluetooth device MAC addresses are randomized before broadcast, including with GAEN, in an effort to prevent a history of the broadcasts by a specific device from being compiled over time.[20]

33. Fourth, the user's phone receives any RPIs and randomized MAC addresses being broadcast by other users' phones within Bluetooth range, [21] which on information and belief, is approximately 30 feet.

---

[16] Apple & Google, *Privacy-Safe Contact Tracing Using Bluetooth Low Energy* 2, https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf (last visited Apr. 27, 2021) [hereinafter *Overview*]; *Bluetooth Specification*, *supra* note 14, at 5; Apple & Google, *Exposure Notifications: Frequently Asked Questions* 3 (Sept. 2020), https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf [hereinafter *FAQ*].

[17] *Bluetooth Specification*, *supra* note 14, at 3, 8; *Overview*, *supra* note 16, at 2.

[18] *FAQ*, *supra* note 16, at 3–4; *Bluetooth Specification*, *supra* note 14, at 5.

[19] *Cryptography Specification*, *supra* note 13, at 5; *Bluetooth Specification*, *supra* note 14, at 5.

[20] *Cryptography Specification*, *supra* note 13, at 5; *Bluetooth Specification*, *supra* note 14, at 5.

[21] *FAQ*, *supra* note 16, at 3–4; *Bluetooth Specification*, *supra* note 14, at 6.

34. The App records all RPIs and MAC addresses the user receives, as well as the user's distance from any RPI's source (that is, from another user's phone), based on the signal strength of the Bluetooth transmission.[22]

35. Fifth, if a GAEN user receives a positive COVID-19 diagnosis, with approval from the local public health authority, the GAEN system will recognize that user's RPIs as coming from an at-risk user.[23]

36. The at-risk users' Keys, which in and of themselves contain no personal information, are marked as exposed and published for anyone to access, by the public health authority.[24]

37. Sixth, the App periodically compares the list of exposed Keys to the list of RPIs the user has come into contact with.[25]

38. Anyone in possession of a Key can calculate which RPIs were generated by it and thereby associate these RPIs with one source known to be a device belonging to a COVID-19 infected individual.[26]

39. If the App determines that the user has come into contact with one or more RPIs generated by an exposed Key, the user is alerted that she has potentially been exposed to the coronavirus.[27]

40. Where GAEN's functionality can be activated without downloading a freestanding App, its inputs and outputs are handled by the device's native software. When GAEN is activated in this way, it otherwise functions in the same way as when it is App-activated.

---

[22] *FAQ*, *supra* note 16, at 7; *Bluetooth Specification*, *supra* note 14, at 6.

[23] *FAQ*, *supra* note 16, at 3–4, 8.

[24] *Bluetooth Specification*, *supra* note 14, at 3; *Cryptography Specification*, *supra* note 13, at 8; *FAQ*, *supra* note 16, at 5.

[25] *FAQ*, *supra* note 16, at 4.

[26] *Bluetooth Specification*, *supra* note 14, at 8 ("A user's Rolling Proximity Identifier changes on average every 15 minutes, and needs the Temporary Exposure Key to be correlated to a contact.").

[27] *FAQ*, *supra* note 16, at 4.

D. GAEN is Supposed to Ensure User Anonymity

41. Through the GAEN system, in theory, the list of RPIs that a user's mobile device sees over time need never leave the device, and users learn from a health authority the set of RPIs that were broadcast by at-risk users, but the identity of those users, and what other users may have also received a broadcast from an at-risk user should remain anonymous. Google represents that GAEN does not share a user's identity; that only public health authorities can use GAEN; and that RPIs never leave a user's phone.[28]

42. Maintaining user privacy and anonymity is important for the Apps. Users trusting that GAEN would not disseminate personal information was critical to attracting sufficiently broad participation for the Apps to play a meaningful role in the public health authorities' COVID-19 responses.[29]

43. Accordingly, Google has represented GAEN's privacy protections as follows:

a. "Doesn't collect personally identifiable information"[30]

b. "List of people you've been in contact with never leaves your phone"[31]

c. "People who test positive are not identified to other users, Google or Apple"[32]

d. "All of the Exposure Notification matching happens on your device."[33]

---

[28] Burke, *supra* note 2; *Overview*, *supra* note 16, at 1.

[29] Pohl & Kasler, *supra* note 8 ("It appears the people most at risk of spreading the disease are not going through the steps that would send an alert. … [T]he app appears to have so far fallen victim to worries about privacy and the pervasiveness of surveillance technology."); Andrew Sheeler, *This App Uses Bluetooth to Tell You If You Have Been Exposed to COVID-19 in California*, The Sacramento Bee, https://www.sacbee.com/news/politics-government/capitol-alert/article247671555.html (Dec. 7, 2020, 5:39 PM) ("'We value privacy, California has long been a leader in terms of advancing the cause and we don't want to do anything to set that cause back,' Newsom said.").

[30] *Overview*, *supra* note 16, at 1.

[31] *Id.*

[32] *Id.*

[33] Google, *supra* note 3.

44. Relying on Google's representations, news media have reported about GAEN as follows:

a. "Apple and Google say they will create software allowing phones to broadcast unique cryptographically generated codes via Bluetooth. The codes won't include identifying information or location data, and the cryptography is designed to make it impossible to tie the codes to a particular person."[34]

b. "Bluetooth-based Covid-19 contact-tracing schemes are designed to upload no data from most users."[35]

c. "Apple and Google emphasize that all of the … privacy protections … . No location data is shared and the system does not share your identity with other users, Apple, or Google. All matching is done on-device and users have full control over whether they want to report a positive test."[36]

45. For devices running Google's Android operating system, Google designed GAEN in a manner that rendered these representations false.

E. Google's Implementation of GAEN Exposes COVID-19 Tracing Data

46. Every Android device hosts a "log file" or "system log": a file for logging important device metrics and events that occur during operation.

47. Smartphone system log files enable application developers, device manufacturers, and/or network providers to obtain necessary data for later analysis, such as to evaluate the stability and reliability of a given application, connection, or device. As such, the system logs

[34] Sidney Fussell & Will Knight, *The Apple–Google Contact Tracing Plan Won't Stop Covid Alone*, Wired (Apr. 14, 2020, 3:04 PM), https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone.

[35] Andy Greenberg, *Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered*, Wired (Apr. 17, 2020, 7:00 AM), https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses.

[36] Chance Miller, *Apple Releases iOS 13.7 with New Built-in COVID-19 Exposure Notifications Express System*, 9 to 5 Mac (Sept. 1, 2020, 1:00 AM), https://9to5mac.com/2020/09/01/covid-19-exposure-ios-13-7-built-in.

exist to transmit information in the logs from the phone to be received by the entities with permission to access the logs.

48. On smartphones running Google's Android operating system, certain applications "pre-installed" on the device (included with the device purchase) are automatically granted permission to access the system logs, called "READ_LOGS" permission.

49. There are hundreds of such applications.

50. Applications with READ_LOGS permission include applications developed by Google (the operating system developer), such as the Android Game Optimizing Service; applications developed by Samsung and Motorola (device manufacturers), such as Samsung's "MyGalaxy" music and video streaming service; and applications developed by AT&T, Verizon, or T-Mobile (mobile network operators), such as Verizon's account management app "MyVerizon."[37]

51. On information and belief, more than one hundred different applications or services that hold READ_LOGS permission and contain code for executing a command to view the system logs can be installed on Android devices.

52. In addition, advertising partners affiliated with entities that have READ_LOGS permissions and third-party software have READ_LOGS permissions in spite of public pronouncements by Google that third parties should not have READ_LOGS permissions.

53. Smartphone system log files may be transmitted to application developers, device manufacturers, and network providers with READ_LOGS permissions in the ordinary course of the phones' operation.[38] Google at times accesses, or has accessed, system log files for upload which contain COVID-19 contact tracing information.

54. Device manufacturer Samsung acknowledges that it collects:

---

[37] With respect to pre-installed applications generally, see Julien Gamba *et al.*, *An Analysis of Pre-installed Android Software* 4–5, 41st IEEE Symposium on Security and Privacy (May 7, 2019), available at https://arxiv.org/pdf/1905.02713.pdf.

[38] Google, *Privacy Security Best Practices*, https://source.android.com/security/best-practices/privacy (Sept. 1, 2020) ("Logging data increases the risk of exposure of that data and reduces system performance. Multiple public security incidents have occurred as a result of logging sensitive user data.").

> information about … your device, including MAC address, IP address, *log information*, device model, hardware model, IMEI number, serial number, subscription information, device settings, connections to other devices, mobile network operator, web browser characteristics, app usage information, sales code, access code, current software version, MNC, subscription information and randomized, non-persistent and resettable device identifiers, such as Personalized Service ID (or PSID), and advertising IDs, including Google Ad ID[.][39]

55. A Samsung-manufactured Android device may have 150 or more pre-installed applications or services that hold READ_LOGS permission and contain code for executing a command to view the system logs.

56. A Motorola-manufactured Android device may have 60 or more pre-installed applications or services that hold READ_LOGS permission and contain code for executing a command to view the system logs.

57. Mobile network operator Verizon acknowledges that "[s]ome Verizon wireless devices include system applications we provide to … collect information about network and device conditions including location, battery life and applications on the device."[40]

58. Mobile network operator T-Mobile acknowledges that it "automatically" collects

> [d]evice and service performance and diagnostic information, including reports from your device about signal strength, speeds, app and service performance, dropped calls, call and data failures, geolocation information, and device data like battery strength and serial number and similar device identifiers, settings, language preferences, and software versions[.][41]

59. System log files may also routinely be transmitted to third parties with READ_LOGS permissions.

---

[39] Samsung, *Samsung Privacy Policy for the U.S.*, https://www.samsung.com/us/account/privacy-policy (Jan. 1, 2021).

[40] Verizon, *Let's Take a Look at the Full Verizon Privacy Policy*, https://www.verizon.com/about/privacy/full-privacy-policy (Apr. 2021).

[41] T-Mobile, *T-Mobile Privacy Notice*, https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (Feb. 23, 2021).

60. Android devices treat the entities with READ_LOGS permission as privileged first parties with respect to device users, as indicated by Google's public explanation that READ_LOGS permissions are "[n]ot for use by third-party applications, because Log entries can contain the user's private information."[42]

61. As Google recognizes, because "logs are a shared resource and are available to an application with the READ_LOGS permission," "inappropriate logging of user information could inadvertently leak user data to other applications."[43]

62. In the mobile application development industry, it is a recognized best practice to log no more than necessary to ensure the application's stability and reliability.[44]

63. In the mobile application development industry, it is a recognized best practice never to log sensitive or personally identifiable information unless the application's basic functionality requires it.[45]

64. Google recognizes and promotes these practices.[46]

65. Google implements GAEN for Android smartphones via its Google Mobile Services, which is a collection Google apps and APIs ("GMS"). Google's GMS instructs, or has instructed, the GAEN system to log every RPI broadcasted and received by the user's phone to the system logs.

66. GAEN logs every COVID-19 exposure notification received by a user to the system logs.

67. On information and belief, GAEN logs every user's input, and failure to input, positive COVID-19 diagnoses to the system logs.

---

[42] Google, *Manifest.permission*, https://developer.android.com/reference/android/Manifest.permission#READ_LOGS (Apr. 21, 2021).

[43] Google, *Security Tips*, https://developer.android.com/training/articles/security-tips (Aug. 7, 2020).

[44] *See, e.g.*, Google, *supra* note 38; Google, *supra* note 43.

[45] *See, e.g.*, Google, *supra* note 38; Google, *supra* note 43.

[46] Google, *supra* note 38; Google, *supra* note 43.

68. Even if GAEN does not log COVID-19 diagnoses to the system logs directly, a positive COVID-19 test result can be inferred from the RPIs that are written to the system logs, because, as discussed *supra*, the Key associated with a positive diagnosis is made publicly available. Anyone can access the publicly-disclosed Key and identify which RPIs were generated by a device belonging to a COVID-19 infected individual.[47]

F. The Exposed COVID-19 Tracing Data is Personally Identifiable

69. The hundreds of applications (and the sophisticated technology companies behind them) with access to system logs can easily associate the data that GAEN logs to the device owner's identity. Device manufacturers, network providers, and application developers commonly already have identifying information about the owners of devices with their apps, or else they have permissions to access information like the phone number associated with a device. Even if they did not, the system logs themselves contain identifying information, including the persistent MAC address associated with the device and the "name" associated with the device (which may contain the user's full name). Other persistent identifiers may also be present in the system logs, such as identifiers associated with specific apps or advertisers. All of this information is available to apps with READ_LOGS permissions.

70. MAC addresses are readily associated with specific locations. For example, an open-source project called Wigle maintains a publicly searchable database associating MAC addresses with specific locations.[48]

71. Thus, contrary to all reasonable expectations and assurances, COVID-19 exposure notifications received by an App user with an Android device, and their own ostensibly anonymous and untraceable report of a positive COVID-19 diagnosis (whether expressly logged or inferred from RPIs), become immediately identifiable when GAEN writes the information to the insecure system logs on Android devices. Upon information and belief, this information is uploaded to numerous third parties and to Google.

---

[47] *Bluetooth Specification*, *supra* note 14, at 8 (explaining that Temporary Exposure Key can "correlate[]" RPIs to a contact).

[48] Wigle, https://wigle.net (last visited Apr. 27, 2021).

72. App users on other devices are also identifiable. The hundreds of third parties with applications that access the system logs can associate the data from other devices that GAEN logs to the owners of those other devices, and can link their RPIs and identities to specific locations. This is because GAEN writes the RPIs received by Android devices to the system logs together with, and directly associated with, the randomized MAC address broadcast by the originating device. Because GAEN logs the randomized MAC addresses and the corresponding RPIs together, the data are formally linked in any collection of the logs.

73. Randomized MAC addresses, like persistent MAC addresses, can be associated with specific locations.[49]

74. Moreover, the randomized MAC addresses associated with a particular user's device are broadcast not just for the Contact Tracing App's purposes, but for all purposes, including Bluetooth device discovery, Bluetooth device usage, and reception by fixed Bluetooth beacons of known location.[50] As such, randomized MAC addresses are routinely made available to entities with an interest in data aggregation. With the benefit of large data sets, these entities can determine identity from randomized MAC addresses and thus it is possible they can link to specific individuals and specific locations the RPIs and other contact tracing information logged by GAEN.

75. Thus, contrary to all reasonable expectations and assurances, any Contact Tracing App user's ostensibly anonymous report of a positive COVID-19 diagnosis can be inferred from RPIs that were supposed to be untraceable, and associated with their identity, and location, if they came, at any time, within Bluetooth range of an App user with an Android device.

76. No aspect of GAEN's functionality requires any of this data to be written to the system logs.

---

[49] *See generally* Jeremy Martin *et al.*, *A Study of MAC Address Randomization in Mobile Devices and When it Fails* (Mar. 31, 2017), available at https://arxiv.org/abs/1703.02874.

[50] Sara Morrison, *Why You See Online Ads for Stuff You Buy in the Real World*, Vox (Jan. 29, 2020, 1:24 PM), https://www.vox.com/recode/2019/12/19/21011527/retail-tracking-apps-wifi-bluetooth-facebook-ads; Ashkan Soltani, *Privacy Trade-offs in Retail Tracking*, Fed. Trade Comm'n (Apr. 30, 2015, 11:59 AM), https://www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking.

G. Millions of App Users Are Affected by the GAEN Security Breach

77. There is no reasonable way for App users to avoid having their personal medical information exposed by the security vulnerabilities that Google designed for GAEN.

78. A representative Android user's experience with GAEN looks as follows: The user downloads and installs or has downloaded a Contact Tracing App on her Samsung Galaxy S10 phone, which came installed with numerous applications, including Facebook, Samsung Pay, Galaxy Store, and Google Chrome apps preinstalled when she bought the phone. Throughout the user's day, the App continuously broadcast the RPIs associated with her device, and recorded RPIs received from other App users who come within Bluetooth range. If the user tests positive for COVID-19, that deeply personal information is entered into the GAEN system. The user believes that her medical information "stays on her device," and that her RPIs cannot be associated with her identity because she has been told so by Google, her public health authority, and the news media. Unbeknownst to her, however, this sensitive data is uploaded by Google, and, on information and belief, by Samsung and dozens of other preinstalled software developers, where it is available to be used to determine, among other things, which other users of GAEN the user has come into contact with, where she has been, and the fact that she has tested positive for COVID-19.

79. A representative Apple iPhone user will also indirectly interact with Google's implementation of GAEN as follows: The user activates GAEN's functionality by navigating to "Settings" on her iPhone11, and clicking a hyperlink that states "Turn On Exposure Notifications." Over the course of her day, she passes by city buses, office buildings, and grocery stores wherein Android device users within Bluetooth range receive RPIs transmitted by her iPhone. Like the Android user, the Apple user believes that the RPIs communicated by GAEN cannot be associated with her identity, and that her potential COVID-19 exposure and status will not be shared without permission. Unbeknownst to her, however, the RPIs her phone transmits are being logged with identifying information by Android devices running GAEN, from which it is communicated to Google and perhaps dozens of other third parties.

H. Google Refuses to Satisfactorily Address this Vulnerability

80. No later than in or about mid-February 2021, Google became aware that COVID-19 contact tracing information had been written to GMS system logs and thus became exposed to any entity having access to those logs. To date, Google has failed to inform the general public or provide widespread notice to GAEN participants of this data security flaw. In or about the third week of April 2021, Google indirectly confirmed the existence of the security flaw by acknowledging that in late March 2021, it began to address the security flaw by rolling out patch fixes. Google continues to keep the general public uninformed about the security flaw and as a result the extent and efficacy of any supposed fixes are unknown to Plaintiffs.

VI. THE NAMED PLAINTIFFS' EXPERIENCES

A. Plaintiff Lewis Bornmann

81. The CA Notify App was downloaded and installed by approximately December 2020 on Plaintiff Bornmann's Android device manufactured by Motorola on T-Mobile's mobile network, and all system settings required for CA Notify to function on his device were enabled.

82. In the interest of preserving his medical privacy, Plaintiff Bornmann does not here recite his COVID-19 status, but states that if he had been positively diagnosed with COVID-19, he would have entered his diagnosis into the CA Notify App.

83. If Plaintiff Bornmann had learned what he now knows about the security of information transmitted by Google's System through CA Notify, he would not have downloaded the app or used it the way he did.

84. On information and belief, system log files from Plaintiff Bornmann's phone have been, and continue to be, received and read by third parties, including Motorola and T-Mobile.

85. On information and belief, system log files from Plaintiffs Bornmann's phone have been, and continue to be, received and read by Google.

B. Plaintiff Jonathan Diaz

86. The CA Notify App was downloaded and installed by approximately December 2020 on Plaintiff Diaz's Android device manufactured by Samsung on Verizon's mobile network, and all system settings required for CA Notify to function on his device were enabled.

87. In the interest of preserving his medical privacy, Plaintiff Diaz does not here recite his COVID-19 status, but states that if he had been positively diagnosed with COVID-19, he would have entered his diagnosis into the CA Notify App.

88. If Plaintiff Diaz had learned what he now knows about the security of information transmitted by Google's System through CA Notify, he would not have downloaded the app or used it the way he did.

89. On information and belief, system log files from Plaintiff Diaz's phone have been received and read by third parties, including Samsung and Verizon.

90. On information and belief, system log files from Plaintiff Diaz's phone have been, and continue to be, received and read by third parties, including Motorola, Samsung, T-Mobile, and Verizon.

91. On information and belief, system log files from Plaintiffs Diaz's phone have been, and continue to be, received and read by Google.

92. Plaintiffs have suffered avoidable invasions of privacy, violations of their dignitary rights, and other significant damages as a result of Google's conduct.

VII. CLASS ACTION ALLEGATIONS

93. Plaintiffs bring this action on behalf of the following Class and Subclasses:

> **Class:** All natural persons in the United States who downloaded or activated a contact tracing app incorporating the Google-Apple Exposure Notification System on their mobile device.
>
> **California Subclass:** All natural persons in California who are members of the Class.

94. Excluded from the Class and Subclasses are Google, its current employees, coconspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies; the undersigned counsel for Plaintiffs and their employees; and the Judge and court staff to whom this case is assigned.

95. The prerequisites to maintaining this action as a class action under Federal Rule of Civil Procedure 23(a) are satisfied.

a. Numerosity: Joinder of all Class Members is impracticable because the

Nationwide and California Classes each encompass millions of individuals, dispersed throughout the United States and California, respectively.

b. Commonality: There are questions of law and fact common to all Plaintiffs and Class Members, including whether and to what extent:

i. Log files containing data created by GAEN from Plaintiffs' and Class Members' mobile devices have been and will be received and read by Google;

ii. Log files containing data created by GAEN from Plaintiffs' and Class Members' mobile devices have been and will be received and read by third parties;

iii. Google made assurances data created by GAEN would not leave users' mobile devices;

iv. Google acted negligently or knowingly;

v. Google's uniform conduct toward each Plaintiff and Class Member violated their statutory, common law, and constitutional rights; and

vi. Google should be enjoined from disclosing Plaintiffs' and Class Members' information.

c. Typicality: Plaintiffs' claims are typical of the other Class Members' because all Class Members were comparably injured through Google's uniform misconduct as described above. Plaintiffs advance the same claims on the same legal theories based on the same facts on behalf of themselves and on behalf of all Class Members.

d. Adequacy: Plaintiffs are adequate representatives because their interests do not conflict with the other Class Members'; Plaintiffs have retained counsel competent and experienced in complex class action litigation; and Plaintiffs intend to prosecute this action vigorously.

96. The prerequisite to maintaining this action as a class action under Federal Rule of Civil Procedure 23(b)(2) is satisfied because in designing, maintaining, and promoting GAEN Google has acted on grounds that apply generally to both Classes.

97. The prerequisites to maintaining this action as a class action under Federal Rule of Civil Procedure 23(b)(3) are satisfied.

a. Predominance: The questions of law and fact common to Class Members predominate over any questions affecting only individual members because Google treated each Plaintiff and Class Member identically in material respects, and most Plaintiffs and Class Members suffered substantially similar injuries.

b. Superiority: A class action is superior to any other available means for adjudicating this controversy because the damages suffered by Plaintiffs and Class Members are relatively small compared to the burden of individually litigating their claims against Google, so it would be virtually impossible for the Class Members to seek redress individually. Even if Class Members could afford it, individual litigation would overwhelm the court system.

VIII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Invasion of Privacy: Public Disclosure of Private Facts

98. Plaintiffs bring this claim on behalf of themselves and the Class.

99. The personal and medical information that Google publicized may be personally identified and includes information about whether they have been exposed to COVID-19, their proximity to other persons and locations over time, and other information from which it can be inferred whether Plaintiffs and Class Members have tested positive for COVID-19.

100. The personal and medical information that Google publicized includes personally identifiable information about whether Plaintiffs and Class Members have tested positive for COVID-19; whether they have been exposed to COVID-19; and information about their proximity to other persons and locations over time.

101. By virtue of exposing Plaintiffs' and Class Members' personal and medical information to potentially hundreds of third party entities, Google allowed that information to escape unfettered into cyberspace, thereby making it available to a number of people so substantial that it is substantially certain to become knowledge readily accessible to the public.

102. A reasonable person in the position of Plaintiffs and Class Members would consider the publicity highly offensive, including because their personal and medical information is inherently sensitive, and because the context and circumstances under which the information

was generated—including in the context of assurances of anonymity and nondisclosure—were inherently private and non-public.

103. There is no legitimate public concern, nor is there any substantial connection to a legitimate public concern, in having Plaintiffs' and Class Members' personal and medical information made generally available to Google or third party data or technology entities. There is only a public concern in keeping such information private in order that it can serve the public interest.

104. Google knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider Plaintiffs' and Class Members' personal and medical information private and non-public, demonstrated by the widespread public expectation, acknowledged and encouraged by Google, that the information would not be disclosed.

105. Google knew, or acted with reckless disregard of the fact, that a reasonable person in the position of Plaintiffs and Class Members would consider the publicity highly offensive, demonstrated by the widespread public expectation, acknowledged and encouraged by Google, that the information would not be disclosed.

106. As a proximate result of such unauthorized disclosures, Plaintiffs and Class Members were harmed because their reasonable expectations of privacy in their personal and medical information was unduly frustrated and thwarted. Google's conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

107. In failing to secure Plaintiffs' and Class Members' personal and Medical Information, and in generating and disclosing Plaintiffs' and Class Members' personal and medical information, Google acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

108. Plaintiffs seek injunctive relief on behalf of the Class, restitution, and all other damages available under this cause of action.

SECOND CLAIM FOR RELIEF

Invasion of Privacy: Intrusion Upon Seclusion

109. Plaintiffs bring this claim on behalf of themselves and the Class.

110. Plaintiffs and Class Members have a reasonable expectation of privacy in the personal and medical information that Google disclosed and shared without authorization, demonstrated by the widespread public expectation, acknowledged and encouraged by Google, that the information would not be disclosed.

111. When Google wrote Plaintiffs' and Class Members' personal and medical information to a location where it was not secure, and disclosed the information to unauthorized persons for unauthorized use, Google invaded Plaintiffs' and Class Members' privacy by, *inter alia*:

a. committing intrusions into Plaintiffs' and Class Members' medical and other private affairs that would be highly offensive to a reasonable person, especially considering the risks to Plaintiffs, Class Members, and society at large that could result from reckless disclosure;

b. committing intrusions into Plaintiffs' and Class Members' medical and other private affairs in a manner that would be highly offensive to a reasonable person, especially considering assurances made and endorsed by Google with respect to the data at issue;

c. accessing private facts concerning Plaintiffs and Class Members without authorization and in contravention of Plaintiffs' and Class Members' reasonable and well-founded expectations; and

d. making available to a large number of third parties private facts concerning Plaintiffs and Class Members without authorization and in contravention of Plaintiffs' and Class Members' reasonable and well-founded expectations.

112. Google knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider Google's actions highly offensive.

113. Google knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider Plaintiffs' and Class Members'

personal and medical information private and non-public, demonstrated by the widespread public expectation, acknowledged and encouraged by Google, that the information would not be disclosed.

114. Google intruded upon Plaintiffs' and California Class Members' sensitive and confidential information in a manner sufficiently serious in nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.

115. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their personal and medical information was unduly frustrated and thwarted. Google's conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

116. In failing to protect Plaintiffs' and Class Members' personal and medical information, and in disclosing Plaintiffs' and Class Members' personal and medical information, Google acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

117. Plaintiffs seek injunctive relief on behalf of the Class, restitution, and all other damages available under this cause of action.

THIRD CLAIM FOR RELIEF

California Constitution, Article 1, § 1

118. Plaintiffs bring this claim on behalf of themselves and the California Subclass.

119. Plaintiffs and California Subclass Members have a legally protected Constitutional privacy interest in the personal and medical information that Google disclosed and shared without authorization, under California Constitution, Article 1, Section 1.

120. Plaintiffs and California Subclass Members reasonably expected that their personal and medical information would not be written to a location where it was not secure, and reasonably expected that under no circumstances would the information be disclosed to unauthorized parties for unauthorized use.

121. Google intruded upon Plaintiffs' and California Subclass Members' sensitive and confidential information in a manner sufficiently serious in nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.

122. Google knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Subclass Members' position would consider Google's actions highly offensive.

123. Google knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Subclass Members' position would consider Plaintiffs' and Subclass Members' personal and medical information private and non-public, demonstrated by the widespread public expectation, acknowledged and encouraged by Google, that the information would not be disclosed.

124. As a proximate result of such unauthorized disclosures, Plaintiffs' and Subclass Members' reasonable expectations of privacy in their personal and medical information was unduly frustrated and thwarted. Google's conduct amounted to a serious invasion of Plaintiffs' and Subclass Members' protected privacy interests.

125. In failing to protect Plaintiffs' and Subclass Members' personal and medical information, and in disclosing Plaintiffs' and Subclass Members' personal and medical information, Google acted with malice and oppression and in conscious disregard of Plaintiffs' and Subclass Members' rights to have such information kept confidential and private.

FOURTH CLAIM FOR RELIEF

California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56 *et seq.*

126. Plaintiffs bring this claim on behalf of themselves and the California Subclass.

127. The California Confidentiality of Medical Information Act (CMIA) prohibits the unauthorized disclosure of medical information; the unauthorized sharing and use of medical information for purposes not necessary to provide healthcare services; the negligent maintenance of medical information; and the negligent release of medical information. Cal. Civ. Code §§ 56.10(a), 56.10(d), 56.10(e), 56.101(a), 56.36(b).

128. Google is subject to the requirements of the CMIA. Cal. Civ. Code §§ 56.10(a), (d), (e); 56.101(a); 56.26(a); 56.36(b).

129. Google is a "Provider of Health Care" under Cal. Civ. Code § 56.06(a)–(b), including because the GAEN endeavor was a business organized for the purpose of maintaining medical information in order to make the information available to an individual for management and/or for diagnosis of potential exposure to COVID-19, and because through GAEN, Google offers software designed to maintain information about whether a user has tested positive for COVID-19 and whether a user has been exposed to COVID-19, in order to make the information available to the user and to California public health authorities, at the request of the user and of California public health authorities, for the treatment and management of COVID-19.

130. Plaintiffs and Subclass Members are "Patients" under Cal. Civ. Code § 56.05(k) because they are natural persons who received health care services, including without limitation COVID-19 exposure notifications and tracing, and to whom the medical information described herein pertains.

131. The log files created by GAEN contain Plaintiffs' and Subclass Members' "Medical Information" under Cal. Civ. Code § 56.05(j) because they contain individually identifiable information about whether Plaintiffs and Subclass Members have tested positive for COVID-19 and about their exposure to COVID-19.

132. Members of the Subclass entered their COVID-19 status into CA Notify, an App that uses GAEN. Google designed GAEN to write that information to the system logs of any such Subclass Member's Android mobile device.

133. Members of the Subclass broadcast their RPIs and randomized MAC addresses to other Subclass Members who used Android devices, and their information was written to the Android device's system logs.

134. The log files created by GAEN are the result of an affirmative communicative act by Google of software design with knowledge that Medical Information contained in the system log files would be communicated to third parties.

135. In violation of Cal. Civ. Code § 56.10(a), Google disclosed Plaintiffs' and Subclass Members' personal and Medical Information without first obtaining authorization.

136. In violation of Cal. Civ. Code § 56.10(d), Google intentionally shared and otherwise used Plaintiffs' and Subclass Members' Medical Information for a purpose not necessary to provide health care services to Plaintiffs or Subclass Members.

137. In violation of Cal. Civ. Code § 56.10(e), Google disclosed Plaintiffs' and Subclass Members' Medical Information to persons or entities which were not engaged in providing direct health care services to Plaintiffs, Subclass Members, their providers of health care, health care service plans, insurers, or self-insured employers.

138. In violation of Cal. Civ. Code § 56.26(a), Google's implementation of GAEN knowingly used, disclosed, and permitted its employees or agents to use or disclose Plaintiffs' and Subclass Members' Medical Information in ways that were not reasonably necessary for Google to perform the functions it provided, including because no aspect of GAEN's functionality required that Plaintiffs' and Subclass Members' Medical Information be written to system logs where they could be acquired by Google and other entities.

139. In violation of the first sentence of Cal. Civ. Code § 56.101(a), Google created, maintained, preserved, and stored Plaintiffs' and Subclass Members' Medical Information in a manner that failed to preserve and breached the confidentiality of the information, including by permitting GAEN to write Medical Information to system log files.

140. Google's violation of the first sentence of Cal. Civ. Code § 56.101(a) was negligent in violation of the second sentence of Cal. Civ. Code § 56.101(a) because Google failed to adhere to best practices in the application development industry and failed to comply with the assurances it made and endorsed with respect to the privacy and security of information stored and transmitted by Apps that implemented GAEN.

141. Google's violations of Cal. Civ. Code § 56.101 caused Plaintiffs' and Subclass Members' Medical Information to be viewed by unauthorized persons.

142. Google negligently released confidential information or records concerning Plaintiffs and Subclass Members—that is, their Medical Information, and other personal information associated with their Medical Information—under Cal. Civ. Code § 56.36(b) in violation of the CMIA.

143. Google's violations of the CMIA caused Plaintiffs' and Subclass Members' Medical Information to be viewed by unauthorized persons.

144. Google acted knowingly and willfully.

145. Google's violations of the CMIA injured Plaintiffs' and Subclass Members' privacy by disclosing their sensitive medical information.

146. Plaintiffs seek injunctive relief on behalf of the Subclass, restitution, statutory damages under Cal. Civ. Code § 56.36(b)(1), and all other damages available under this cause of action.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs ask that the Court enter the following:

A. An order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are Class Representatives, that Plaintiffs' attorneys shall be appointed as Class Counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

B. Judgment against Google for Plaintiffs' and Class Members' asserted claims for relief;

C. Equitable and injunctive relief (1) enjoining Google from including from continuing to copy Plaintiffs' and Class Members' personal and medical information to the system logs on Android devices and from continuing to allow unauthorized parties access to Plaintiffs' and Class Members' personal and medical information in the system logs, (2) requiring Google to ensure that all personal and medical information acquired, created, or otherwise obtained from the system logs is destroyed, and (3) and as otherwise just and proper;

D. An order awarding Plaintiffs and the Class Members actual and/or statutory and/or special and/or incidental damages and restitution;

E. An order requiring Google to pay punitive damages and exemplary damages;

F. An order requiring Google to pay pre-judgment and post-judgment interest;

G. Reasonable attorney's fees and costs reasonably incurred; and

H. Any and all other and further relief to which Plaintiffs and the Class or Subclasses

may be entitled.

X. DEMAND FOR JURY TRIAL

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

Dated: April 27, 2021

Respectfully Submitted,

/s/ Michael W. Sobol

Michael W. Sobol (SBN 194857)
msobol@lchb.com
Melissa Gardner (SBN 289096)
mgardner@lchb.com
Ian Bensberg (SBN *pro hac vice pending*)
ibensberg@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

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