

1 LIEFF CABRASER HEIMANN & BERNSTEIN, LLP  
Michael W. Sobol (SBN 194857)  
2 Melissa Gardner (SBN 289096)  
Ian Bensberg (*pro hac vice pending*)  
3 275 Battery Street, 29<sup>th</sup> Floor  
San Francisco, CA 94111-3339  
4 (415) 956-1000

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

10 *Attorneys for Plaintiffs and the Proposed Class*

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**Page**

I. INTRODUCTION ..... 1

II. PARTIES ..... 2

III. JURISDICTION..... 2

IV. INTRADISTRICT ASSIGNMENT..... 2

V. GOOGLE’S CONDUCT ..... 3

    A. Background: The COVID-19 Pandemic ..... 3

    B. Google’s Exposure Notification System..... 3

    C. How GAEN Works ..... 5

    D. GAEN is Supposed to Ensure User Anonymity ..... 8

    E. Google’s Implementation of GAEN Exposes COVID-19 Tracing Data ..... 9

    F. The Exposed COVID-19 Tracing Data is Personally Identifiable..... 13

    G. Millions of App Users Are Affected by the GAEN Security Breach ..... 15

    H. Google Refuses to Satisfactorily Address this Vulnerability..... 16

VI. THE NAMED PLAINTIFFS’ EXPERIENCES ..... 16

    A. Plaintiff Lewis Bornmann ..... 16

    B. Plaintiff Jonathan Diaz..... 16

VII. CLASS ACTION ALLEGATIONS ..... 17

VIII. CLAIMS FOR RELIEF ..... 19

    FIRST CLAIM FOR RELIEF

        Invasion of Privacy: Public Disclosure of Private Facts ..... 19

    SECOND CLAIM FOR RELIEF

        Invasion of Privacy: Intrusion Upon Seclusion ..... 21

    THIRD CLAIM FOR RELIEF

        California Constitution, Article 1, § 1..... 22

    FOURTH CLAIM FOR RELIEF

        California Confidentiality of Medical Information Act, Cal. Civ. Code

            §§ 56 *et seq.* ..... 23

IX. PRAYER FOR RELIEF..... 26

X. DEMAND FOR JURY TRIAL..... 27

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 Mobile Services, a collection of Google apps and APIs (“GMS”). Google unequivocally  
6 assures that it completely safeguards the sensitive information necessarily involved with COVID-  
7 19 contact tracing. However, because Google’s implementation of GAEN allows this sensitive  
8 contact tracing data to be placed on a device’s system logs and provides dozens or even hundreds  
9 of third parties access to these system logs, Google has exposed GAEN participants’ private  
10 personal and medical information associated with contact tracing, including notifications to  
11 Android device users of their potential exposure to COVID-19.

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

19 The exposed information is personally identifiable. The contact tracing apps themselves  
20 generate ostensibly-secure personal device identifiers, which change periodically as they are  
21 broadcast to other devices, and should be traceable to the device user only with a “key” held by  
22 the public health authorities. But in storage, these identifiers are maintained alongside other  
23 device identifiers known as MAC addresses. When this stored data is written to mobile device  
24 system logs, it becomes available to third parties with access to the logs. They, alone or in  
25 concert, can use the MAC addresses to trace the identifiers back to individual identities, locations,  
26 and other identifying attributes, effectively creating an alternative “key” of their own. For those  
27 who have reported testing positive, it enables third parties to link that diagnosis back to the  
28 particular patient, defeating the purported anonymity Google claims for its service.

1 In February 2021, Google was informed of the security flaw in its implementation of  
2 GAEN that caused the data breach alleged herein. To date, Google has failed to inform the public  
3 that participants in GAEN have had their private personal and medical information exposed to  
4 third parties, who in the ordinary course of business may access the system logs from time to  
5 time, or that Google itself may access these logs.

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

11 **II. PARTIES**

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

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

14 3. Defendant Google LLC (“Google”) is a Delaware Limited Liability Company  
15 based at 1600 Amphitheatre Way, Mountain View, California, whose sole member is XXVI  
16 Holdings Inc. XXVI Holdings Inc. is a corporation incorporated in Delaware with its principal  
17 office in California.

18 **III. JURISDICTION**

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

22 **IV. INTRADISTRICT ASSIGNMENT**

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

1 **V. GOOGLE’S CONDUCT**

2 **A. Background: The COVID-19 Pandemic**

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

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

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

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

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

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

16 **B. Google’s Exposure Notification System**

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

19 13. In May 2020, Google implemented GAEN and made it available to public health  
20 authorities worldwide.<sup>2</sup>

21 14. GAEN acts a framework or platform on which a public health authority can build a  
22 mobile contact tracing application (“Contact Tracing App” or “App”) for use in its jurisdiction.<sup>3</sup>

23  
24 \_\_\_\_\_  
25 <sup>1</sup> 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).

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

28 <sup>3</sup> Google, *Exposure Notifications*, <https://www.google.com/covid19/exposurenotifications> (last visited Apr. 27, 2021).

1 15. Google advertises its implementation of GAEN as “[u]sing technology to help  
2 public health authorities fight COVID-19.”<sup>4</sup>

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

8 17. In the United States, more than 28 million people, residents of each jurisdiction  
9 above, have downloaded Contact Tracing Apps that use GAEN or activated exposure  
10 notifications on their mobile devices.<sup>6</sup>

11 18. California’s Contact Tracing App is called CA Notify and was developed by the  
12 California Department of Technology.<sup>7</sup>

13 19. Users of Apple devices in California may activate the functionality of CA Notify  
14 on their phones without having to download the App.<sup>8</sup>

15 20. CA Notify has been downloaded to about 9.5 million mobile devices.<sup>9</sup>

16 21. CA Notify has been downloaded to about 8.5 million Apple devices.<sup>10</sup>

---

17  
18 <sup>4</sup> *Id.*

19 <sup>5</sup> Mishaal Rahman, *Here Are the Countries Using Google and Apple’s COVID-19 Contact*  
20 *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>.

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

23 <sup>7</sup> Cal., *California Can Stop the Spread*, <https://canotify.ca.gov/> (last visited Apr. 27, 2021); Cal.  
24 *Dep’t of Technology, CA Notify*,  
<https://play.google.com/store/apps/details?id=gov.ca.covid19.exposurenofications> (Apr. 5,  
25 2021).

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

28 <sup>9</sup> *Id.*

<sup>10</sup> *Id.* (“about nine times as many people have enrolled in CA Notify on an iPhone”).

1 22. CA Notify has been downloaded to about 1 million Android devices.<sup>11</sup>

2 **C. How GAEN Works**

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

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

11 25. Second, as part of the activation process, GAEN generates a unique, random-  
12 seeming sequence of characters called a Temporary Exposure Key (“Key”) for the user.<sup>13</sup>

13 26. A new Key is generated once every 24 hours after installation.<sup>14</sup>

14 27. Third, the App uses the Key to generate a “rolling proximity identifier key,” which  
15 then generates a different, unique, random-seeming sequence of characters called a “rolling  
16 proximity identifier” (RPI).<sup>15</sup>

17  
18  
19 

---

<sup>11</sup> *Id.*

20 <sup>12</sup> Russell Brandom, *Apple and Google Announce New Automatic App System to Track COVID*  
21 *Exposures*, The Verge (Sept. 1, 2020, 12:00 PM),  
22 [https://www.theverge.com/2020/9/1/21410281/apple-google-coronavirus-exposure-notification-](https://www.theverge.com/2020/9/1/21410281/apple-google-coronavirus-exposure-notification-contact-tracing-app-system)  
23 [contact-tracing-app-system](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*  
24 *Android Phone*, <https://support.google.com/android/answer/9888358> (last visited Apr. 27, 2021)  
25 (“To use the system, you need to download an official app from your region’s government public  
26 health authority.”).

27 <sup>13</sup> Apple & Google, *Exposure Notification: Cryptography Specification 6* (Apr. 23, 2020),  
28 [https://blog.google/documents/69/Exposure\\_Notification\\_-](https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf)  
29 [\\_Cryptography\\_Specification\\_v1.2.1.pdf](https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf) [hereinafter *Cryptography Specification*].

30 <sup>14</sup> Apple & Google, *Exposure Notification: Bluetooth Specification 3* (Apr. 23, 2020),  
31 [https://blog.google/documents/70/Exposure\\_Notification\\_-](https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf)  
32 [\\_Bluetooth\\_Specification\\_v1.2.2.pdf](https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf)  
33 [hereinafter *Bluetooth Specification*].

34 <sup>15</sup> *Cryptography Specification*, *supra* note 13, at 6–7.

1           28.     As the user goes about her day, her phone broadcasts the RPI over its Bluetooth  
2 radio to other users' phones within range, whose devices receive and record the broadcasted  
3 incoming RPI.<sup>16</sup>

4           29.     The App generates a new RPI for the user's phone every 15 or 20 minutes.<sup>17</sup>

5           30.     The App records all the RPIs it broadcasts.<sup>18</sup>

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

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

15           33.     Fourth, the user's phone receives any RPIs and randomized MAC addresses being  
16 broadcast by other users' phones within Bluetooth range,<sup>21</sup> which on information and belief, is  
17 approximately 30 feet.

---

21           <sup>16</sup> Apple & Google, *Privacy-Safe Contact Tracing Using Bluetooth Low Energy 2*,  
22 [https://blog.google/documents/57/Overview\\_of\\_COVID-19\\_Contact\\_Tracing\\_Using\\_BLE.pdf](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;  
23 Apple & Google, *Exposure Notifications: Frequently Asked Questions* 3 (Sept. 2020),  
24 <https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf> [hereinafter *FAQ*].

25           <sup>17</sup> *Bluetooth Specification*, *supra* note 14, at 3, 8; *Overview*, *supra* note 16, at 2.

26           <sup>18</sup> *FAQ*, *supra* note 16, at 3–4; *Bluetooth Specification*, *supra* note 14, at 5.

27           <sup>19</sup> *Cryptography Specification*, *supra* note 13, at 5; *Bluetooth Specification*, *supra* note 14, at 5.

28           <sup>20</sup> *Cryptography Specification*, *supra* note 13, at 5; *Bluetooth Specification*, *supra* note 14, at 5.

<sup>21</sup> *FAQ*, *supra* note 16, at 3–4; *Bluetooth Specification*, *supra* note 14, at 6.



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

4           35.     Fifth, if a GAEN user receives a positive COVID-19 diagnosis, with approval  
5 from the local public health authority, the GAEN system will recognize that user's RPIs as  
6 coming from an at-risk user.<sup>23</sup>

7           36.     The at-risk users' Keys, which in and of themselves contain no personal  
8 information, are marked as exposed and published for anyone to access, by the public health  
9 authority.<sup>24</sup>

10          37.     Sixth, the App periodically compares the list of exposed Keys to the list of RPIs  
11 the user has come into contact with.<sup>25</sup>

12          38.     Anyone in possession of a Key can calculate which RPIs were generated by it and  
13 thereby associate these RPIs with one source known to be a device belonging to a COVID-19  
14 infected individual.<sup>26</sup>

15          39.     If the App determines that the user has come into contact with one or more RPIs  
16 generated by an exposed Key, the user is alerted that she has potentially been exposed to the  
17 coronavirus.<sup>27</sup>

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

21  
22 \_\_\_\_\_  
<sup>22</sup> *FAQ*, *supra* note 16, at 7; *Bluetooth Specification*, *supra* note 14, at 6.

23 <sup>23</sup> *FAQ*, *supra* note 16, at 3–4, 8.

24 <sup>24</sup> *Bluetooth Specification*, *supra* note 14, at 3; *Cryptography Specification*, *supra* note 13, at 8;  
25 *FAQ*, *supra* note 16, at 5.

26 <sup>25</sup> *FAQ*, *supra* note 16, at 4.

27 <sup>26</sup> *Bluetooth Specification*, *supra* note 14, at 8 (“A user's Rolling Proximity Identifier changes on  
28 average every 15 minutes, and needs the Temporary Exposure Key to be correlated to a  
contact.”).

<sup>27</sup> *FAQ*, *supra* note 16, at 4.

1           **D.     GAEN is Supposed to Ensure User Anonymity**

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

8           42.     Maintaining user privacy and anonymity is important for the Apps. Users trusting  
9 that GAEN would not disseminate personal information was critical to attracting sufficiently  
10 broad participation for the Apps to play a meaningful role in the public health authorities’  
11 COVID-19 responses.<sup>29</sup>

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

- 13           a.     “Doesn’t collect personally identifiable information”<sup>30</sup>  
14           b.     “List of people you’ve been in contact with never leaves your phone”<sup>31</sup>  
15           c.     “People who test positive are not identified to other users, Google or  
16 Apple”<sup>32</sup>  
17           d.     “All of the Exposure Notification matching happens on your device.”<sup>33</sup>

18  
19  
20           <sup>28</sup> Burke, *supra* note 2; *Overview*, *supra* note 16, at 1.

21           <sup>29</sup> Pohl & Kasler, *supra* note 8 (“It appears the people most at risk of spreading the disease are not  
22 going through the steps that would send an alert. ... [T]he app appears to have so far fallen victim  
23 to worries about privacy and the pervasiveness of surveillance technology.”); Andrew Sheeler,  
24 *This App Uses Bluetooth to Tell You If You Have Been Exposed to COVID-19 in California*, The  
25 Sacramento Bee, [https://www.sacbee.com/news/politics-government/capitol-  
alert/article247671555.html](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.”).

26           <sup>30</sup> *Overview*, *supra* note 16, at 1.

27           <sup>31</sup> *Id.*

28           <sup>32</sup> *Id.*

<sup>33</sup> Google, *supra* note 3.

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

3           a. “Apple and Google say they will create software allowing phones to  
4 broadcast unique cryptographically generated codes via Bluetooth. The codes won’t include  
5 identifying information or location data, and the cryptography is designed to make it impossible  
6 to tie the codes to a particular person.”<sup>34</sup>

7           b. “Bluetooth-based Covid-19 contact-tracing schemes are designed to upload  
8 no data from most users.”<sup>35</sup>

9           c. “Apple and Google emphasize that all of the ... privacy protections ... . No  
10 location data is shared and the system does not share your identity with other users, Apple, or  
11 Google. All matching is done on-device and users have full control over whether they want to  
12 report a positive test.”<sup>36</sup>

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

15           **E. Google’s Implementation of GAEN Exposes COVID-19 Tracing Data**

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

18           47. Smartphone system log files enable application developers, device manufacturers,  
19 and/or network providers to obtain necessary data for later analysis, such as to evaluate the  
20 stability and reliability of a given application, connection, or device. As such, the system logs  
21  
22

---

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

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

27 <sup>36</sup> Chance Miller, *Apple Releases iOS 13.7 with New Built-in COVID-19 Exposure Notifications*  
28 *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>.

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

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

6 49. There are hundreds of such applications.

7 50. Applications with READ\_LOGS permission include applications developed by  
8 Google (the operating system developer), such as the Android Game Optimizing Service;  
9 applications developed by Samsung and Motorola (device manufacturers), such as Samsung's  
10 "MyGalaxy" music and video streaming service; and applications developed by AT&T, Verizon,  
11 or T-Mobile (mobile network operators), such as Verizon's account management app  
12 "MyVerizon."<sup>37</sup>

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

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

19 53. Smartphone system log files may be transmitted to application developers, device  
20 manufacturers, and network providers with READ\_LOGS permissions in the ordinary course of  
21 the phones' operation.<sup>38</sup> Google at times accesses, or has accessed, system log files for upload  
22 which contain COVID-19 contact tracing information.

23 54. Device manufacturer Samsung acknowledges that it collects:

24 \_\_\_\_\_  
25 <sup>37</sup> With respect to pre-installed applications generally, see Julien Gamba *et al.*, *An Analysis of*  
26 *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>.

27 <sup>38</sup> Google, *Privacy Security Best Practices*, [https://source.android.com/security/best-](https://source.android.com/security/best-practices/privacy)  
28 [practices/privacy](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.").

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

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

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

13 57. Mobile network operator Verizon acknowledges that “[s]ome Verizon wireless  
14 devices include system applications we provide to ... collect information about network and  
15 device conditions including location, battery life and applications on the device.”<sup>40</sup>

16 58. Mobile network operator T-Mobile acknowledges that it “automatically” collects  
17 [d]evice and service performance and diagnostic information,  
18 including reports from your device about signal strength, speeds,  
19 app and service performance, dropped calls, call and data failures,  
20 geolocation information, and device data like battery strength and  
21 serial number and similar device identifiers, settings, language  
22 preferences, and software versions[.]<sup>41</sup>

21 59. System log files may also routinely be transmitted to third parties with  
22 READ\_LOGS permissions.  
23

24  
25 <sup>39</sup> Samsung, *Samsung Privacy Policy for the U.S.*, <https://www.samsung.com/us/account/privacy-policy> (Jan. 1, 2021).

26 <sup>40</sup> Verizon, *Let’s Take a Look at the Full Verizon Privacy Policy*,  
27 <https://www.verizon.com/about/privacy/full-privacy-policy> (Apr. 2021).

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

1           60.     Android devices treat the entities with READ\_LOGS permission as privileged first  
2 parties with respect to device users, as indicated by Google’s public explanation that  
3 READ\_LOGS permissions are “[n]ot for use by third-party applications, because Log entries can  
4 contain the user’s private information.”<sup>42</sup>

5           61.     As Google recognizes, because “logs are a shared resource and are available to an  
6 application with the READ\_LOGS permission,” “inappropriate logging of user information could  
7 inadvertently leak user data to other applications.”<sup>43</sup>

8           62.     In the mobile application development industry, it is a recognized best practice to  
9 log no more than necessary to ensure the application’s stability and reliability.<sup>44</sup>

10          63.     In the mobile application development industry, it is a recognized best practice  
11 never to log sensitive or personally identifiable information unless the application’s basic  
12 functionality requires it.<sup>45</sup>

13          64.     Google recognizes and promotes these practices.<sup>46</sup>

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

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

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

---

22  
23 <sup>42</sup> Google, *Manifest.permission*,  
24 [https://developer.android.com/reference/android/Manifest.permission#READ\\_LOGS](https://developer.android.com/reference/android/Manifest.permission#READ_LOGS) (Apr. 21,  
2021).

25 <sup>43</sup> Google, *Security Tips*, <https://developer.android.com/training/articles/security-tips> (Aug. 7,  
26 2020).

27 <sup>44</sup> *See, e.g.*, Google, *supra* note 38; Google, *supra* note 43.

28 <sup>45</sup> *See, e.g.*, Google, *supra* note 38; Google, *supra* note 43.

<sup>46</sup> Google, *supra* note 38; Google, *supra* note 43.

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

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

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

17           70. MAC addresses are readily associated with specific locations. For example, an  
18 open-source project called Wigle maintains a publicly searchable database associating MAC  
19 addresses with specific locations.<sup>48</sup>

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

26 \_\_\_\_\_  
27 <sup>47</sup> *Bluetooth Specification*, *supra* note 14, at 8 (explaining that Temporary Exposure Key can  
"correlate[]" RPIs to a contact).

28 <sup>48</sup> Wigle, <https://wisle.net> (last visited Apr. 27, 2021).



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

8           73. Randomized MAC addresses, like persistent MAC addresses, can be associated  
9 with specific locations.<sup>49</sup>

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

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

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

---

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

26 <sup>50</sup> Sara Morrison, *Why You See Online Ads for Stuff You Buy in the Real World*, Vox (Jan. 29,  
27 2020, 1:24 PM), [https://www.vox.com/recode/2019/12/19/21011527/retail-tracking-apps-wifi-](https://www.vox.com/recode/2019/12/19/21011527/retail-tracking-apps-wifi-bluetooth-facebook-ads)  
28 [bluetooth-facebook-ads](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-](https://www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking)  
[events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking](https://www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking).



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

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

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

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

1           **H.     Google Refuses to Satisfactorily Address this Vulnerability**

2           80.     No later than in or about mid-February 2021, Google became aware that COVID-  
3     19 contact tracing information had been written to GMS system logs and thus became exposed to  
4     any entity having access to those logs. To date, Google has failed to inform the general public or  
5     provide widespread notice to GAEN participants of this data security flaw. In or about the third  
6     week of April 2021, Google indirectly confirmed the existence of the security flaw by  
7     acknowledging that in late March 2021, it began to address the security flaw by rolling out patch  
8     fixes. Google continues to keep the general public uninformed about the security flaw and as a  
9     result the extent and efficacy of any supposed fixes are unknown to Plaintiffs.

10          **VI.    THE NAMED PLAINTIFFS' EXPERIENCES**

11           **A.     Plaintiff Lewis Bornmann**

12           81.     The CA Notify App was downloaded and installed by approximately December  
13     2020 on Plaintiff Bornmann's Android device manufactured by Motorola on T-Mobile's mobile  
14     network, and all system settings required for CA Notify to function on his device were enabled.

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

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

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

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

25           **B.     Plaintiff Jonathan Diaz**

26           86.     The CA Notify App was downloaded and installed by approximately December  
27     2020 on Plaintiff Diaz's Android device manufactured by Samsung on Verizon's mobile network,  
28     and all system settings required for CA Notify to function on his device were enabled.

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

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

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

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

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

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

16 **VII. CLASS ACTION ALLEGATIONS**

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

18                   **Class:** All natural persons in the United States who downloaded or  
19 activated a contact tracing app incorporating the Google-Apple  
Exposure Notification System on their mobile device.

20                   **California Subclass:** All natural persons in California who are  
21 members of the Class.

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

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

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

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

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

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

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

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

11 iv. Google acted negligently or knowingly;

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

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

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

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

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

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

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

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

10 **VIII. CLAIMS FOR RELIEF**

11 **FIRST CLAIM FOR RELIEF**

12 **Invasion of Privacy: Public Disclosure of Private Facts**

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

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

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

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

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

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

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

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

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

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

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

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

27  
28

**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'

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

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

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

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

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

17 **THIRD CLAIM FOR RELIEF**

18 **California Constitution, Article 1, § 1**

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

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

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

27  
28



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

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

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

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

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

19 **FOURTH CLAIM FOR RELIEF**

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

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

22 127. The California Confidentiality of Medical Information Act (CMIA) prohibits the  
23 unauthorized disclosure of medical information; the unauthorized sharing and use of medical  
24 information for purposes not necessary to provide healthcare services; the negligent maintenance  
25 of medical information; and the negligent release of medical information. Cal. Civ. Code  
26 §§ 56.10(a), 56.10(d), 56.10(e), 56.101(a), 56.36(b).

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

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

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

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

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

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

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

26           135. In violation of Cal. Civ. Code § 56.10(a), Google disclosed Plaintiffs’ and  
27 Subclass Members’ personal and Medical Information without first obtaining authorization.  
28

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

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

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

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

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

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

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

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

3 144. Google acted knowingly and willfully.

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

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

9 **IX. PRAYER FOR RELIEF**

10 WHEREFORE, Plaintiffs ask that the Court enter the following:

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

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

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

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

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

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

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

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

1 may be entitled.

2 **X. DEMAND FOR JURY TRIAL**

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

4

5 Dated: April 27, 2021

Respectfully Submitted,

6

/s/ Michael W. Sobol

7

Michael W. Sobol (SBN 194857)

msobol@lchb.com

8

Melissa Gardner (SBN 289096)

mgardner@lchb.com

9

Ian Bensberg (SBN *pro hac vice pending*)

ibensberg@lchb.com

10

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

275 Battery Street, 29th Floor

11

San Francisco, CA 94111-3339

Telephone: 415.956.1000

12

Facsimile: 415.956.1008

13

Nicholas Diamand (*pro hac vice pending*)

ndiamand@lchb.com

14

Douglas Cuthbertson (*pro hac vice pending*)

dcuthbertson@lchb.com

15

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

250 Hudson Street, 8<sup>th</sup> Floor

16

New York, NY 10013

Telephone: 212.355.9500

17

Facsimile: 212.355.9592

18

19

20

21

22

23

24

25

26

27

28

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

Diaz, Jonathan; Bornmann, Lewis

(b) County of Residence of First Listed Plaintiff Alameda County, California (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

(see attachment)

DEFENDANTS

Google LLC

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff 3 Federal Question (U.S. Government Not a Party) 2 U.S. Government Defendant 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, OTHER, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding 2 Removed from State Court 3 Remanded from Appellate Court 4 Reinstated or Reopened 5 Transferred from Another District (specify) 6 Multidistrict Litigation-Transfer 8 Multidistrict Litigation-Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. § 1332(d)(2)

Brief description of cause:

Privacy violations under common law, California Confidentiality of Medical Information Act, and California Constitution

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$

CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only)

SAN FRANCISCO/OAKLAND

X SAN JOSE

EUREKA-MCKINLEYVILLE

DATE 04/27/2021

SIGNATURE OF ATTORNEY OF RECORD

/s/ Michael W. Sobol

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

**ATTACHMENT A  
ATTORNEYS FOR PLAINTIFFS**

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

Michael W. Sobol (SBN 194857)

msobol@lchb.com

Melissa Gardner (SBN 289096)

mgardner@lchb.com

Ian R. Bensberg

ibensberg@lchb.com

275 Battery Street, 29th Floor

San Francisco, CA 94111-3339

Telephone: (415) 956-1000

Facsimile: (415) 956-1008

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

Nicholas Diamand

ndiamand@lchb.com

Douglas Cuthbertson

dcuthbertson@lchb.com

250 Hudson Street, 8th Floor

New York, NY 10013

Telephone: (212) 355-9500

Facsimile: (212) 355-9592