WILLKIE FARR & GALLAGHER LLP
Benedict Y. Hur (SBN: 224018)
Simona Agnolucci (SBN: 246943)
Eduardo E. Santacana (SBN: 281668)
Tiffany Lin (SBN: 321472)
One Front Street, 34th Floor
San Francisco, CA 94111
Telephone: (415) 858-7400
Facsimile: (415) 858-7599
bhur@willkie.com
sagnolucci@willkie.com
esantacana@willkie.com
tlin@willkie.com

Attorneys for
GOOGLE LLC

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,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Case No. 5:21-cv-03080 NC

DEFENDANT GOOGLE LLC's NOTICE OF MOTION AND MOTION TO DISMISS COMPLAINT PURSUANT TO FED. R. CIV. P. 12(B)(1) AND 12(B)(6)

Judge: Hon. Nathanael Cousins
Court: Courtroom 5 – 4th Floor
Date: August 4, 2021
Time: 1:00 p.m.

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE THAT, on August 4, 2021 at 1:00 p.m., the undersigned will appear before the Honorable Nathanael Cousins of the United States District Court for the Northern District of California at the San Jose Courthouse, Courtroom 5, 4th Floor, 280 South 1st Street, San Jose, CA 95113, and shall then and there present Defendant Google LLC ("Google")'s Motion to Dismiss ("Motion").

Google brings this Motion under Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure. Google will, and hereby does, move for an order dismissing the Complaint with prejudice because any amendment of the Complaint would be futile. The Motion is based on this Notice of Motion and Motion, the following Memorandum of Points and Authorities, Request for Judicial Notice and exhibits attached thereto, the pleadings and other papers on file in this action, any oral argument, and any other evidence that the Court may consider in hearing this Motion.

ISSUES PRESENTED

Whether Plaintiffs' Complaint should be dismissed for lack of subject-matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1) where Plaintiffs lack Article III standing, whether Plaintiffs' Complaint should be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted, and whether the Complaint should be dismissed with prejudice where amendment would be futile.

WILLKIE FARR & GALLAGHER LLP

Date: June 29, 2021

By: */s/ Benedict Y. Hur*
Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Tiffany Lin

Attorneys for Defendant
Google LLC

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

In early 2020, as the world was grappling with the COVID-19 pandemic, Google and Apple, Inc. teamed up to develop technology to meet the needs of public health authorities to quickly and efficiently conduct contact tracing in order to slow the spread of COVID-19. The resulting Exposure Notification ("EN") system was developed with robust privacy protections in place. Over the past year, the EN system has been used by millions of users and dozens of public health authorities around the world. Google and Apple made the technology available free of charge.

Apparently no good deed goes unpunished. Plaintiffs Jonathan Diaz and Lewis Bornmann do not allege that any bad actor has accessed, viewed, disclosed, or used their information as a result of the EN system; they instead merely allege it is theoretically possible that someone *could*. In other words, this is a case about a hypothetical and exceedingly unlikely risk of harm. Plaintiffs' Complaint is noticeably devoid of factual allegations showing that an individual's use of the EN system was ever used to identify an individual, and the explanations for how that might be possible are convoluted and highly theoretical. Google now moves to dismiss Plaintiffs' Complaint with prejudice because: (1) Plaintiffs have failed to establish Article III standing; (2) Plaintiffs cannot state a claim for privacy violations under California common law, the California Constitution, or the California Confidentiality of Medical Information Act ("CMIA"); and (3) any amendment of the Complaint would be futile.

II. BACKGROUND

A. Relevant Procedural History

Plaintiffs filed their Class Action Complaint on April 27, 2021, alleging the following claims: (1) public disclosure of private facts; (2) intrusion upon seclusion; (3) violation of Article I, Section 1 of the California Constitution; and (4) violation of the CMIA. ECF 1. The initial case management conference is set for July 28, 2021. ECF 4 at 2.

B. Relevant Factual Background

1. Exposure Notification System

On April 10, 2020, Google and Apple announced an Exposure Notification ("EN") system that uses Bluetooth technology on mobile devices to aid in contact tracing efforts.[1] ECF 1 ¶¶ 6–13. The goal of the project is to assist public health authorities in their efforts to fight COVID-19 by enabling exposure notifications in a privacy-preserving manner.[2] Google and Apple have released software tools called Application Programming Interfaces ("APIs") that enable public health authorities to build mobile applications to help with COVID-19 contact tracing efforts across Android and iOS devices in a privacy-protective way.[3] The EN system can be used only to support approved contact tracing apps of authorized public health authorities.[4] Some public health authorities have built apps that use the EN system, some use a template app developed and supported by Google, and other public health authorities offer contact tracing using the EN system without creating an app (CA Notify on iOS devices is one example).[5] ECF 1 ¶¶ 17–24. In all cases, in order to enable the EN system, the user must activate exposure notifications and consent to the terms and conditions of their public health authority's contact-tracing app or services. ECF 1 ¶¶ 17–24. Google and Apple committed to not monetizing the EN system, and to disabling the EN system on a regional basis when it is no longer needed.[6]

Once EN is enabled by the user, the user's device will regularly send out a beacon via Bluetooth that includes a Rolling Proximity Identifier ("RPI"): a string of random numbers that aren't tied to a user's identity and that changes every 15 to 20 minutes.[7] ECF 1 ¶¶ 25–33. When

[1] *See* Google's RJN Ex. 1, *Use the COVID-19 Exposure Notifications System on your Android phone*, Google Play Help, https://support.google.com/googleplay/answer/9888358?hl=en (last visited June 7, 2021); Google's RJN Ex. 2, *Exposure Notifications: Using technology to help public authorities fight COVID-19*, Google COVID-19 Information and Resources, https://www.google.com/covid19/exposurenotifications/ (last visited June 7, 2021); Google's RJN Ex. 3, *Exposure Notifications: Frequently Asked Questions*, September 2020 v1.2, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf.
[2] *See* Google's RJN Ex. 3.
[3] *Id.*
[4] *Id.*
[5] *Id.*; Google's RJN Ex. 1.
[6] Google's RJN Ex. 3.
[7] *Id.*

another phone with the EN system enabled receives an RPI, it will store that RPI on the device.[8] *Id.* ¶ 27. The device also generates a Temporary Exposure Key ("TEK") that changes every 24 hours. *Id.* ¶¶ 26, 28, 29. Neither RPIs nor TEKs contain personal information. *Id.* ¶ 36. RPIs and TEKs are stored on users' devices, and after 14 days the data is deleted.[9] Android devices contain a temporary memory buffer that contains a few hours' worth of data and is primarily accessible to and used for debugging purposes by a limited number of pre-installed applications with specific permission granted by device manufacturers.[10]

If a user receives a positive COVID-19 test result, the local public health authority can provide the user with a verification code to submit that test result in the health authority's app. *Id.* ¶ 35. After the test result is entered, the EN system enables the user to choose to upload the TEKs generated over the last 14 days on their device. *Id.* ¶ 35. Public health authorities designate a server to maintain a list of TEKs associated with users who have reported a positive test result. *Id.* ¶ 36. Apps using the EN system periodically download and compare the list of TEKs of users who have reported a positive test result to the list of RPIs each user has come into contact with over the past 14 days. *Id.* ¶ 37. If the system determines that a user has come into contact with an RPI generated by a TEK associated with a user who submitted a positive test result, the health authority's app can display an exposure notification to the potentially exposed user. *Id.* ¶ 39. The exposure notification alerts the potentially exposed user that they have recently come in contact with someone who has tested positive for COVID-19 and provides the health authority's guidance on next steps.[11] The EN system shares with the health authority the day the contact occurred, how long it lasted, the Bluetooth signal strength of that contact, and the type of report that confirmed the positive test result.[12]

---

[8] *Id.*

[9] Google's RJN Ex. 4: *CA Notify: Apps on Google Play*, Google Play, https://play.google.com/store/apps/details?id=gov.ca.covid19.exposurenotifications (last visited June 7, 2021).

[10] The memory buffer is temporary; it is of limited size, so data is cleared from it on a rolling basis once new data is written to the log. Typically, the memory buffer contains data from only the last few hours.

[11] Google's RJN Ex. 3.

[12] *Id.*

CA Notify is California's official implementation of the EN system. The CA Notify Privacy Policy provides that the following categories of de-identified data may be processed and collected by CA Notify: (1) Installing and deleting the app (Android only); (2) Enabling and disabling exposure notifications; (3) Receiving an exposure notification; (4) Entering a verification code to send anonymous keys; (5) Anonymous keys that have been voluntarily shared.[13] The policy states, "[t]he data may also be shared with local public health authorities and the University of California. This information will not include any personal or location information, nor can it be used to identify any system user."[14] The policy also provides that, though a user's identity is not shared, "[i]t is possible that someone who receives an exposure notice could guess the identity of the COVID-19 positive individual, if they had a limited number of contacts on a given day."[15]

2. Plaintiffs' Allegations

Plaintiffs allege that every Android device hosts a "system log" wherein the EN system records exposure notifications, as well as "every user's input, and failure to input, positive COVID-19 diagnoses to the system logs." ECF 1 ¶¶ 46, 66, 67. Plaintiffs allege that certain applications on Android devices, as well as third-party entities affiliated with those apps, have permission to access the system logs. *Id.* ¶¶ 48–53. Plaintiffs also allege that device manufacturers and mobile network operators may collect information from the system logs. *Id.* ¶¶ 54–58. Finally, Plaintiffs allege that the entities with access to the system logs "can easily associate the data that [the EN system] logs to the device owner's identity." *Id.* ¶ 69. Plaintiffs allege that users of non-Android devices are harmed because "the RPIs [the non-Android users' devices] transmit[] are being logged with identifying information by Android devices running [the EN system], from which it is communicated to Google and perhaps dozens of other third parties." *Id.* ¶ 79.

---

[13] Google's RJN Ex. 5, *Privacy Policy*, CA Notify, https://covid19.ca.gov/notify-privacy/ (last updated Mar. 23, 2021).

[14] *Id.*

[15] *Id.* Public health authorities that use Google's EN service must comply with the Google COVID-19 Exposure Notifications Service Additional Terms as well as Google's API Terms of Service. *Google COVID-19 Exposure Notifications Service Additional Terms* (May 4, 2020), https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf.

Plaintiffs allege that Named Plaintiffs Lewis Bornmann and Jonathan Diaz downloaded and activated the CA Notify App on Android devices in December 2020. *Id.* ¶¶ 81, 86. Plaintiffs do not allege whether Bornmann or Diaz entered a positive test result into the CA Notify App, nor whether they interacted with the App in any way after installing and activating the app.[16] *Id.* ¶¶ 82–85, 87–92. Plaintiffs purport to represent a class of "[a]ll 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," with a subclass of "[a]ll natural persons in California who are members of the Class." *Id.* ¶ 93.

Plaintiffs state that Google began "rolling out patch fixes" to "address the security flaw" in late March 2021. *Id.* ¶ 80.

III. LEGAL STANDARD

A. Rule 12(b)(1)

Federal courts are courts of limited jurisdiction and are presumptively without jurisdiction. *See Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994).[17] Federal Rule of Civil Procedure 12(b)(1) allows a defendant to move to dismiss a claim for lack of subject-matter jurisdiction. Fed. R. Civ. P. 12(b)(1). It is the plaintiff's burden to establish the existence of subject-matter jurisdiction in response to a Rule 12(b)(1) motion. *See Kingman Reef Atoll Inv., LLC v. United States*, 541 F.3d 1189, 1197 (9th Cir. 2008).

"[L]ack of Article III standing requires dismissal for lack of subject matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1)." *Naruto v. Slater*, 888 F.3d 418, 425 n.7 (9th Cir. 2018). A named plaintiff purporting to represent a class must establish Article III standing; otherwise, he cannot "seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494–95 (1974). To establish Article III standing, the plaintiff must show: "(1) a concrete and particularized injury, that (2) is fairly traceable to the challenged conduct, and (3) is likely to be redressed by a favorable decision." *Virginia House of Delegates v.*

[16] Plaintiffs chose not to seek to file any portion of the Complaint under seal or seek to use pseudonyms in place of their actual names.

[17] Internal citations and quotation marks have been omitted and emphases added unless otherwise noted.

Bethune-Hill, 139 S. Ct. 1945, 1950 (2019). The injury must be "(a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). A plaintiff "must show standing with respect to each form of relief sought." *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 978 (9th Cir. 2011). Standing for injunctive relief requires a plaintiff to show "continuing, present adverse effects" or a "sufficient likelihood that [the plaintiff] will again be wronged in a similar way." *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1119–20 (9th Cir. 2020). Standing for damages requires more than a mere risk of future harm. *TransUnion LLC v. Ramirez*, No. 20-297, slip op. at 20–21 (U.S. June 25, 2021). "Article III standing requires a concrete injury even in the context of a statutory violation." *Id.* at *8. "Under Article III, federal courts do not adjudicate hypothetical or abstract disputes." *Id.* at *6.

B. Rule 12(b)(6)

A motion to dismiss for failure to state a claim under Rule 12(b)(6) tests the legal sufficiency of the complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). To survive a motion to dismiss under Rule 12(b)(6), a plaintiff must plead facts showing that his right to relief rises above "the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," and pleadings that are "no more than conclusions, are not entitled to the assumption of truth." *Ashcroft v. Iqbal*, 556 U.S. 662, 678–79 (2009). A court need not accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008).

Dismissal without leave to amend is appropriate if "amendment would be futile." *Carrico v. City & Cnty. of San Francisco*, 656 F.3d 1002, 1008 (9th Cir. 2011). An amendment is futile when "no set of facts can be proved under the amendment to the pleadings that would constitute a valid and sufficient claim or defense." *Miller v. Rykoff-Sexton, Inc.*, 845 F.2d 209, 214 (9th Cir. 1988).

IV. ARGUMENT

A. Plaintiffs lack Article III standing.

Plaintiffs lack Article III standing because their alleged injury (1) is highly speculative; (2)

is not fairly traceable to the challenged conduct; (3) would not be redressed by a favorable decision; and (4) is not sufficiently particularized.[18]

First, Plaintiffs cannot show that they have suffered, or will imminently suffer, an injury in fact. Plaintiffs' argument rests on the highly speculative fear that, despite the clearing of data from the temporary memory buffer on a rolling basis, the limited access to the memory buffer and TEK list, the regeneration of random TEKs every 24 hours and random RPIs every 15 minutes, and the various privacy policies and protections in place, "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."[19] ECF 1 ¶ 75.

Plaintiffs' theory of standing "relies on a highly attenuated chain of possibilities, [and] does not satisfy the requirement that threatened injury must be certainly impending." *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 410 (2013). As the Supreme Court reiterated just last week, "[b]ecause no evidence in the record establishes a serious likelihood of disclosure, we cannot simply presume a material risk of concrete harm." *TransUnion LLC*, No. 20-297, slip op. at 23; *cf. In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598–99 (9th Cir. 2020) (finding standing where Plaintiffs alleged Facebook directly correlated users' personally identifiable browsing history with users' personal Facebook profiles). As to Plaintiffs' arguments regarding risk of future harm, Plaintiffs have not provided facts sufficient to establish that the "risk of harm is sufficiently imminent and substantial" as would be required for injunctive relief. *TransUnion*

---

[18] Because each of the Named Plaintiffs has alleged the same set of facts regarding their interactions with the EN system and the CA Notify app, Google addresses the Rule 12(b)(1) analysis for both Named Plaintiffs together.

[19] As the sources Plaintiffs cite in their Complaint demonstrate, only public health authorities have access to the EN system, and only EN-compliant apps receive TEKs from the diagnosis server. *See* ECF 1. n. 13 at 8 (*Cryptography Specification*: "The Diagnosis Server aggregates the Diagnosis Keys from all users who have tested positive, and distributes them to all the user clients that are participating in exposure notification."); *id.* n.16 at 5 (FAQ: "Access to the technology will be granted only to public health authorities. If they create an app, it must meet specific criteria around privacy, security, and data control. The public health authority will be able to access a list of beacons provided by users confirmed as positive for COVID-19 who have consented to sharing them."). The Complaint alleges that "[t]he 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." ECF 1 ¶ 36. Nowhere does the Complaint contradict, however, the cited documentation, which clarifies that only the app run by the public health authority learns the TEK list, not the user.

LLC, No. 20-297, slip op. at 20. Indeed, Plaintiffs acknowledge that Google began addressing the alleged issue through patch fixes starting in late March 2021. ECF 1 ¶ 80. And, as to Plaintiffs' request for damages, Plaintiffs have not demonstrated that the risk of future harm (that a third party accessed their information) materialized, nor that other class members were even aware of or harmed by their exposure to the risk itself. *See TransUnion LLC*, No. 20-297, at 22–23.

Plaintiffs cannot establish Article III standing because they have not alleged facts sufficient to allege disclosure of their information to a third party, nor harm resulting from that disclosure. "For a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party. . . . If no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated." *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1088 (E.D. Cal. 2015) (finding no standing to bring claims of invasion of privacy or breach of confidentiality where the plaintiff failed to "allege[] facts from which a plausible inference could be drawn that [someone] has viewed his PII/PHI as a result of the Data Breach."); *see also TransUnion LLC*, No. 20-297, at 19 ("The mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm.").

Indeed, courts have repeatedly held that in order to establish Article III standing to assert privacy claims under California law, it is not enough for Plaintiffs to plead that their personal information was collected; they must also allege that their personal information was wrongfully *disclosed*. *See Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1050 (N.D. Cal. 2018); *see also Bassett v. ABM Parking Servs., Inc.*, 883 F.3d 776, 778 (9th Cir. 2018) (holding that the plaintiff failed to allege an injury for purposes of Article III where plaintiff did not allege that anyone viewed, stole, or otherwise used his private credit card information). Furthermore, unauthorized disclosure in and of itself, with a conjectural or hypothetical threat of future harm, does not confer standing. *See In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 977–78 (N.D. Cal. 2014); *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011) (finding no credible, real, and immediate threat of harm where a digital service provider was alleged to have disclosed information to unauthorized third parties); *Yunker v. Pandora Media*

Inc., No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) (finding insufficient harm to confer standing where Pandora shared personal information without anonymizing it).

Second, Plaintiffs fail to plead facts sufficient to allege that their hypothetical injury is fairly traceable to the challenged conduct. Plaintiffs have not alleged that they entered any information into the CA Notify app. Plaintiffs also have not alleged any facts showing that their information has been misused in any way after activating the app, nor that they have received any indication their information has been accessed or viewed by an unauthorized third party. *See, e.g.*, *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1036 (N.D. Cal. 2019) (holding that Plaintiff Bass failed to demonstrate a plausible link to the data breach despite showing that he received spam e-mails on his Facebook account).

Third, Plaintiffs cannot show that their alleged injury is likely to be redressed by a favorable decision. Plaintiffs allege that "Google's [Google Mobile Services] instructs, or has instructed, the GAEN system to log every RPI broadcasted and received by the user's phone to the system logs," and that "a positive COVID-19 test result can be inferred from the RPIs that are written to the system logs." ECF 1 ¶¶ 65, 68. Plaintiffs request injunctive relief "(1) enjoining Google from including [sic] 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." ECF 1 at 26. But Plaintiffs also acknowledge that, in March 2021, Google began rolling out patch fixes to address the very issue of which Plaintiffs complain, and merely plead ignorance about whether Google has since fixed the alleged issue. *See* ECF 1 ¶ 80. Plaintiffs cannot seek prospective relief without specifically alleging an ongoing violation of law, and their Complaint pointedly declines to do that. And, regardless, because Plaintiffs cannot show disclosure or harm, as described above, they are not entitled to damages under any of the asserted privacy claims.

Finally, Plaintiffs have not established that the alleged injury is "sufficiently particularized." *Jewel v. National Security Agency*, 673 F.3d 902, 909 (9th Cir. 2011). Plaintiffs' allegations relate only to Google's practices generally, and the allegations that third parties can

potentially access their information are speculative and weak. Plaintiffs have not alleged that they entered COVID diagnoses or received exposure notifications from the CA Notify app. Nor have Plaintiffs alleged that their specific information was disclosed to third parties as a result of Google's alleged practices. *Cf. Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1021 (N.D. Cal. 2012) (finding that plaintiffs articulated, with particularity, injury as to themselves where plaintiffs gave specific examples of their information that was allegedly transmitted to third parties).

Plaintiffs' allegations are insufficient to establish Article III standing; therefore, Plaintiffs cannot seek relief on behalf of themselves or any other member of the proposed class. The Court should not "abandon [its] usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors." *Clapper*, 568 U.S. at 414. The Complaint should be dismissed for lack of Article III standing under Federal Rule of Civil Procedure 12(b)(1).

B. Plaintiffs fail to state a claim upon which relief can be granted.

1. Plaintiffs fail to state a claim for public disclosure of private facts because there was no public disclosure.

For a common-law public disclosure of private facts claim, a plaintiff must allege disclosure to the public "at large." *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1062 (N.D. Cal. 2014). In *Opperman*, the court dismissed the public disclosure claim where plaintiffs alleged that their phone address books were transmitted in an unencrypted manner, or over public Wi-Fi, "making [them] publicly available to third parties as well as service providers." *Opperman*, 87 F. Supp. 3d at 1062. The court reasoned that the plaintiffs failed to meet the disclosure requirement because "[w]hile Plaintiffs alleged that their information could have been intercepted by third parties, they do not allege that any interception occurred, nor do they allege that it was 'substantially certain' that their address books would become 'public knowledge.'" *Id.* In the instant case, Plaintiffs have alleged even fewer facts that could lead to an inference of public disclosure "at large" of "private facts."

First, there is no allegation of any public disclosure. Plaintiffs have alleged that the RPIs, MAC addresses, and COVID test results *could be* viewed by a limited number of third-party entities, such as device manufacturers, but fail to allege that any information related to an

individual's use of the EN System was actually viewed, or that any of these entities were even aware of the information being included in the system log.

Second, even if this information had been disclosed, Plaintiffs allege that disclosure would only have been to entities that were provided access to the system log by device manufacturers, rather than to the public at large. *See* ECF 1 ¶ 72. Plaintiffs have not alleged that members of the general public outside this limited number of app developers or device manufacturers would even be able to access, view, or piece together this information to reveal a person's "private facts," or that it is "substantially certain" members of the general public would do so. Indeed, to allege that this information was publicly available, Plaintiffs would have had to allege an improbable series of events: that members of the general public (i) knew what these MAC addresses and RPIs are; (ii) hacked into users' devices to find them; (iii) found a way to gain access to access-restricted TEK lists; and then (iv) matched them up to COVID test results and personally identifying information.

Finally, anonymized RPIs and MAC addresses are not "private facts" because they do not reveal any non-public identifying information about the user. *See, e.g.*, *Taus v. Loftus*, 40 Cal. 4th 683, 717–18 (2007) (stating that private facts constitute sufficiently sensitive or intimate details of plaintiffs' lives).

2. Plaintiffs fail to state a claim for intrusion upon seclusion or invasion of privacy because the alleged intrusion was not intentional or highly offensive.

A claim for intrusion upon seclusion under California common law requires a showing that "(1) a defendant 'intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy[,]' and (2) the intrusion 'occur[red] in a manner highly offensive to a reasonable person." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 601. "The intrusion must be intentional." *Varnado v. Midland Funding LLC*, 43 F. Supp. 3d 985, 992 (N.D. Cal. 2014). "Effective consent negates an intrusion upon seclusion claim." *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016).

A plaintiff alleging an invasion of privacy under the California Constitution must show that "(1) they possess a legally protected privacy interest, (2) they maintain a reasonable

expectation of privacy, and (3) the intrusion is 'so serious. . . as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 601. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 37 (1994). "The California Constitution . . . set[s] a high bar for an invasion of privacy claim."[20] *Low*, 900 F. Supp.2d at 1025. "Even negligent conduct that leads to theft of highly personal information, including social security numbers, does not 'approach [the] standard' of actionable conduct under the California Constitution." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012); *see also Razuki v. Caliber Home Loans, Inc.*, No. 17cv1718-LAB (WVG), 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (dismissing California Constitution invasion of privacy claim because plaintiff's allegations "don't suggest the type of intentional, egregious privacy invasion contemplated" by case law).

Because the tests for intrusion upon seclusion and invasion of privacy are so similar, "courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 601.

First, Plaintiffs have not pled any facts showing that, if any intrusion occurred, such intrusion was intentional. The facts alleged in Plaintiffs' Complaint show that the EN system was set up with the purpose of providing a benefit to society in the midst of a global pandemic, and with the goal of enabling contact tracing in a privacy-protective manner. Indeed, all the outside sources provided by Plaintiffs (Google requests judicial notice of a few of them), indicate that Google set the EN system up with every intention of ensuring that *no* intrusion or invasion of privacy would occur.[21] Plaintiffs also allege that, only a few weeks after Google allegedly became aware of the issue, Google "began to address the security flaw by rolling out patch fixes."[22] The

[20] It would be rare for a disclosure that does not violate the CMIA to violate a patient's constitutional right to privacy. *Garrett v. Young*, 109 Cal. App. 4th 1393, 1410 (2003); *see infra* Section IV.B.3.
[21] *See* Google's RJN Exs. 1–3.
[22] ECF 1 ¶ 80.

facts alleged in Plaintiffs' Complaint show the opposite of intent. *See Razuki*, 2018 WL 2761818, at *2 (holding that "[plaintiff's] allegations don't suggest the type of intentional, egregious privacy invasion contemplated" by California case law where plaintiff alleged defendant failed to protect his personal data by choosing to implement low-budget security measures). Claims 2 and 3 therefore fail as a matter of law and cannot be plausibly amended.

Second, any intrusion into Plaintiffs' *de-identified* data would not be highly offensive because Plaintiffs, through enabling exposure notifications and activating the CA Notify app, understand that RPIs will be stored on their own devices and broadcast and exchanged with other participating devices. For those who test positive and choose to share their test result, they understand that the health authority's app will send out exposure notifications based on the sharing of that information, and also understand the possibility that their identity could be guessed by a party who receives the notifications, if those receiving the notifications have had a limited number of contacts on a given day.[23]

In the instant case, users of CA Notify are aware that when the app is enabled, their RPIs and TEKs are being collected by other devices. The potential access or disclosure of randomized RPI information by an app developer, or a device manufacturer, would not be highly offensive where Plaintiffs understand that the same information will be broadcast from their phones to nearby devices. *See Opperman*, 87 F. Supp. 3d at 1059 ("the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant.").

Third, any intrusion would not be "highly offensive" because Plaintiffs have not alleged facts showing that third-party entities or members of the general public have gained unwanted access to their test results or the exposure notifications Plaintiffs received. Plaintiffs theorize that third parties could, through a series of hypothetical steps, identify users using the randomized strings of characters and numbers generated by the EN apps, but "it is not clear that anyone has

[23] *See e.g.*, Google's RJN Ex. 5; Privacy Policy, Connecticut State Connecticut COVID-19 Response (October 30, 2020), https://portal.ct.gov/Coronavirus/COVIDAlertCT/PrivacyPolicy; MD Covid Alert Privacy Policy, Maryland Department of Health CovidLINK, https://covidlink.maryland.gov/content/mdcovidalert/privacy-policy/ (last visited June 26, 2021).

actually done so, or what information, precisely, these third parties have obtained." *Low*, 900 F. Supp. 2d at 1025; *see also In re Zoom Video Comms. Inc. Privacy Litig.*, No. 20-CV-02155-LHK, 2021 WL 930623, at *15 (N.D. Cal. Mar. 11, 2021) (dismissing plaintiffs' invasion of privacy claim because "[p]laintiffs fail to allege that Zoom actually shared *their* personal data with third parties"); *cf. McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1035 (N.D. Cal. 2019) ("Plaintiffs state in detail what data was secretly collected, how the collection was done, and how the harvested data was used.").

The RPIs, TEKs, and MAC addresses allegedly disclosed to third parties consist of randomized strings of numbers and characters; that information, without more, hardly constitutes an "egregious breach of social norms" or a "serious invasion" of a privacy interest. *See Low*, 900 F. Supp. 2d at 1025 (holding that Plaintiffs failed to state a claim for invasion of privacy where LinkedIn allegedly disclosed to third parties the numeric code associated with a user and the URL of the profile page used, and that there was no evidence third parties de-anonymized this data to obtain personal information); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 (holding that the alleged disclosure of unique device identifier number, personal data, and geolocation information from Plaintiffs' Apple devices did not constitute an egregious breach of privacy under the California Constitution); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 987–88 (N.D. Cal. 2014) (holding that plaintiffs' allegations that user data was disclosed to third-party developers contrary to Google's own policies failed to meet the high bar for intrusion upon seclusion). The hypothetical disclosure of randomized strings of numbers and characters, which alone cannot be used to identify an individual, falls far below the high standard necessary to state a claim for intrusion upon seclusion or invasion of privacy.

3. Plaintiffs fail to state a claim under the CMIA because Google is not a provider of health care and Plaintiffs' medical information has not been collected, disclosed, or viewed.

The CMIA, Cal. Civ. Code §§ 56 *et seq.*, prohibits a provider of health care from disclosing, either purposefully or negligently, medical information without the patient's consent. Cal. Civ. Code §§ 56.10, 56.101.

a. Google is not a provider of health care under the CMIA.

The CMIA's definition of "provider of health care" includes the following:

> (a) Any business organized for the purpose of maintaining medical information, as defined in subdivision (j) of Section 56.05, in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care . . . .
>
> (b) Any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information, as defined in subdivision (j) of Section 56.05, in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care . . . .

Cal. Civ. Code §§ 56.06(a)–(b).

Plaintiffs have not alleged facts sufficient to establish that Google is a provider of health care as defined by the CMIA. Plaintiffs simply make the following conclusory statement:

> 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.

ECF 1 ¶ 129.

First, it is unclear whether Plaintiffs are alleging that it is Google or the EN system (or what Plaintiffs call the "GAEN endeavor") that is the "business" contemplated in Civ. Code §§ 56.06(a)–(b). *See id.* As to Google, Plaintiffs have pled no facts alleging that Google is a "business organized for the purpose of maintaining medical information" as required by Civ. Code § 56.06(a). Google also does not meet the requirements of Section 56.06(b) because Google is a technology provider that built functionality in APIs for public health authorities to use to configure and deploy contact-tracing solutions with health authorities' branding for use by

members of the public.[24] As to the EN system, that system is a technology, not a business. Though the term "business" is not defined in the CMIA, the State of California Franchise Tax Board considers a person to be "doing business" when they meet any of the following: (1) "Engage in any transaction for the purpose of financial gain within California"; (2) "Are organized or commercially domiciled in California"; or (3) "Your California sales, property or payroll exceed the following amounts . . . ."[25] Plaintiffs have not alleged that Google and Apple developed the EN system for financial gain, and Google and Apple have disclosed to the public that they developed the technology for the purpose of assisting public health authorities with contact tracing.[26] ECF 1 at 1. Plaintiffs have not alleged that the EN system is organized or commercially domiciled in California, nor that it makes sales, owns property, or provides payroll.

Second, Plaintiffs have failed to allege facts sufficient to establish that the EN system was "organized for the purpose of" or "designed to maintain medical information." The CMIA defines the term "medical information" as follows:

> any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment. 'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

Civ. Code § 56.05. The CMIA's definition of "medical information" has two necessary elements: (1) "individually identifiable information," i.e., information that "alone or in combination with other publicly available information, reveals the individual's identity," and (2) information regarding "a patient's medical history, mental or physical condition, or treatment." *See* Civ. Code § 56.05. Any one element, by itself, is insufficient: "This definition does not encompass demographic or numeric information that does not reveal medical history, diagnosis, or care."

---

[24] *See, e.g.*, Google RJN Ex. 4.
[25] *Doing Business in California*, State of California Franchise Tax Board, https://www.ftb.ca.gov/file/business/doing-business-in-california.html#:~:text=If%20you%20are%20doing%20business,or%20commercially%20domiciled%20in%20California (last visited May 28, 2021).
[26] Google RJN Ex. 3.

Eisenhower Med. Ctr. v. Superior Court, 226 Cal. App. 4th 430, 435 (2014). In other words, release of individually identifiable information in and of itself (such as the fact that a patient visited a certain doctor or clinic) is insufficient to violate the statute. *Id.* at 435. "[T]he mere fact that a person is or was a patient is not accorded the same level of privacy as more specific information about his medical history." *Id.* at 436.

The purpose of the EN system, as Plaintiffs acknowledge, was to *avoid* maintenance of "individually identifiable information" coupled with information about an individual's "medical history, diagnosis, or care." Plaintiffs allege "Google represents that GAEN does not share a user's identity" and "Google has represented [that GAEN d]oesn't collect personally identifiable information." ECF 1 ¶¶ 41, 43. As Plaintiffs' allegations demonstrate, the EN system was not organized for the purpose of maintaining medical information; quite the opposite, it was designed to privately conduct contact tracing and to delete such information from phones after 14 days.

Third, Plaintiffs have failed to allege facts sufficient to establish that the EN system was created "in order to make the [medical] information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual." Cal. Civ. Code §§ 56.06(a), 56.06(b). Civ. Code §§ 56.06(a) and 56.06(b) were added to the CMIA in 2013 to clarify that personal health records, such as those offered as an application by a commercial vendor of personal health service software to allow an individual to monitor and manage his or her own medical information, are also subject to CMIA protections. A.B. 658, Assem. Com. on Jud., at 4–5 (Ca. 2013). The legislative history makes clear that the amendments were not intended to apply to "all medical information, broadly construed, that is created by the individual," such as pedometer data generated by a fitness application; rather, the intent was to "protect medical information that originated with medical professionals, whether providers, insurers, administrators, or other contractors who held a person's medical information." *Id.* Contact-tracing applications using the EN system, akin to the fitness applications that collect information that does not originate with medical professionals, are the types of applications to which the CMIA was *not* intended to apply.

Plaintiffs have stated that the purpose of the EN system was to make medical information (which, as previously discussed, requires individually identifiable 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." ECF 1 ¶ 129.[27] The very documents that Plaintiffs reference in their Complaint, and of which Google requests judicial notice, contradict this statement.[28] As previously discussed, the EN system was organized specifically *not* to collect or maintain individually identifiable information. Additionally, the EN system was created for the purpose of warning *other* users of potential COVID-19 exposure, not for "the diagnosis and treatment of the individual" where "individual" refers to the user of the app. The EN system cannot diagnose an individual with COVID, nor treat a COVID-positive individual. Because Plaintiffs fail to allege facts sufficient to establish that Google, the app, or the EN system is a "provider of health care," Plaintiffs cannot state a claim for violation of the CMIA.

b. The app does not collect medical information, nor have Plaintiffs input medical information into the app.

Even assuming that Google meets the definition of "health care provider," any information collected by the EN system does not meet the definition of medical information; thus, Plaintiffs cannot state a claim under the CMIA.

The randomized identifiers—RPIs, TEKs, and MAC addresses—are random strings of characters and numbers, periodically regenerated so as to minimize the likelihood that they would be used to identify an individual. And Plaintiffs have not alleged that exposure notifications alone can be used to identify an individual. As previously discussed, the CMIA's definition of "medical information" contains two necessary elements: 1) individually identifiable information and 2) information about medical history, diagnosis, or care. *See, e.g.*, *Eisenhower*, 226 Cal. App. 4th at

[27] Paragraph 129 of the Complaint appears to assume that "California public health authorities" would be considered "provider[s] of health care" under the CMIA; however, Plaintiffs do not provide any facts to explain how "California public health authorities" meet any of the CMIA's definitions of "provider of health care," including as defined under Sections 56.05(m), 56.06(a), or 56.06(b). See, e.g., Cal. Civ. Code § 56.06(a) ("Any business organized for the purpose of maintaining medical information . . . in order to make the information available to an individual or to a provider of health care").

[28] *See* Google's RJN Exs. 1–3 (discussing the intent of the EN system to avoid collection of individually identifying information, such as user identity).

435; Civ. Code § 56.05. The randomized identifiers and exposure notifications alone cannot be used to identify an individual, nor have Plaintiffs alleged that anyone has used these randomized identifiers or exposure notifications in such a way as to actually identify individuals.

Plaintiffs also failed to allege that they provided information about their medical history, diagnosis, or care to the app. Plaintiffs have not alleged that they have submitted a COVID-positive test result through the app.[29] Without that, Plaintiffs cannot plead a violation of the CMIA because none of their medical information would have been available to be disclosed. Simply downloading and activating the app, without more, does not provide the app with any information about the user's medical history, diagnosis, or care. Thus, even assuming that personally identifiable information was disclosed (as explained above, it was not), Plaintiffs have not pled that they supplied a COVID test result through the app and thus have failed to plead a violation of the CMIA.

c. Plaintiffs have not pled that disclosure of medical information occurred under section 56.10.

Civil Code section 56.10 prohibits health care providers from "disclos[ing]" medical information. The word "disclose" requires a plaintiff to plead an "affirmative communicative act" by the defendant, more than just making medical information accessible via the Internet. *Stasi v. Inmediata Health Group Corp.*, No. 19cv2353 JM (LL), 2020 WL 6799437, at *14 (S.D. Cal. Nov. 19, 2020). Rather, a plaintiff must allege that the defendant intentionally posted their information, or did some other affirmative act with intent to communicate that information. *Id.*

Even assuming that Google meets the definition of "health care provider," Plaintiffs have not alleged that Google took an "affirmative communicative act" with intent to communicate the medical information, as required by Section 56.10. As previously discussed, the facts alleged in the Complaint lead to the opposite conclusion—that any medical information, if disclosed, was

[29] Though Plaintiffs allege that COVID exposure notifications are logged by the EN system, Plaintiffs have not alleged that they received any exposure notifications, and even if they did, an exposure notification in and of itself would not constitute information "regarding a patient's medical history, mental or physical condition, or treatment" as contemplated by the CMIA.

not done so intentionally. Therefore, Plaintiffs cannot plead a violation of Section 56.10 of the CMIA.

d. Plaintiffs have not alleged that the medical information was viewed by an unauthorized person, as required by sections 56.101 and 56.36.

Section 56.101 of the CMIA provides that any health care provider "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." In order to state a claim under Sections 56.101 and 56.36 of the CMIA, a plaintiff must allege that the medical information was viewed by an unauthorized person. *Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1555 (2014). If no unauthorized person has viewed the medical information, no confidentiality breach has occurred. *Id.* at 1557.

As previously discussed, Google is not a health care provider as defined by the CMIA. Even assuming that Google meets the definition of "health care provider," Plaintiffs have not alleged that the medical information was viewed by an unauthorized person, as required by Sections 56.101 and 56.36. *Id.* at 1555. In *Sutter Health*, a computer with medical information stored on it was stolen. However, there was no allegation that the thief—or anyone else—had viewed the medical information on the hard drive. The court concluded that, even if Sutter had been negligent in storing the medical information on the computer, without an allegation that an unauthorized person had viewed the records (and that confidentiality was breached), there is no negligent release in violation of Sections 56.101 and 56.36 of the CMIA, and there is no remedy, even for nominal damages. *Id.* at 1557–59. In the instant case, Plaintiffs allege that their RPI and MAC addresses are exposed to third parties and that certain third parties may be able to match RPIs to individuals. That is completely speculative. There is no allegation that anyone has viewed and matched any COVID-19 diagnosis or exposure to any individual. Plaintiffs cannot state a claim for a violation of Sections 56.101 and 56.36 of the CMIA.

C. Amendment would be futile.

Plaintiffs should not be given leave to amend their Complaint where, as here, amendment would be futile. Because Plaintiffs have failed to provide facts sufficient to demonstrate that the

alleged issue still exists, Plaintiffs cannot carry their burden of establishing subject-matter jurisdiction. And Plaintiffs cannot plead any facts regarding access, viewing, or disclosure of their information, as required to state a claim for the alleged violations of their privacy rights. For these reasons, Plaintiffs' Complaint should be dismissed without leave to amend.

V. CONCLUSION

The Complaint consists of allegations that never rise beyond the level of mere speculation. Plaintiffs do not allege any facts showing that a third party accessed, viewed, disclosed, or used their information, nor that they were injured, or even likely to be injured, by the alleged issue of which they complain. Plaintiffs also fail to demonstrate that the alleged issue still exists. It is Plaintiffs' burden to establish that subject-matter jurisdiction exists and to provide facts sufficient to state a claim upon which relief can be granted. Plaintiffs have done neither. The Complaint should be dismissed with prejudice pursuant to Rules 12(b)(1) and 12(b)(6).]

WILLKIE FARR & GALLAGHER LLP

Date: June 29, 2021

By: */s/ Benedict Y. Hur*
Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Tiffany Lin

Attorneys for Defendant
Google LLC