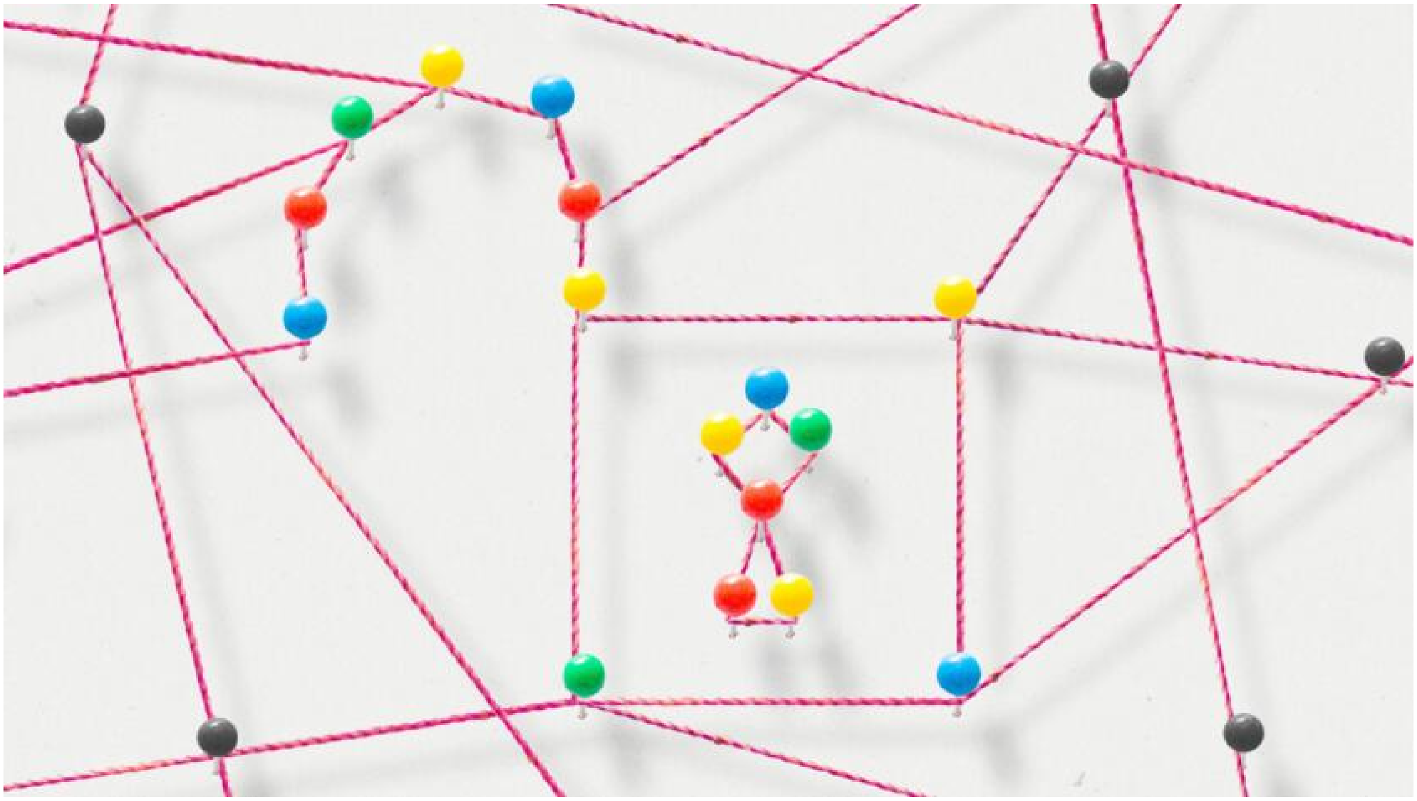
The Markup

# Google Promised Its Contact Tracing App Was Completely Private—But It Wasn’t

By Alfred Ng

April 27, 2021 08:00 ET

Viewable online at
https://themarkup.org/privacy/2021/04/27/google-promised-its-contact-tracing-app-was-completely-private-but-it-wasnt



Google's contact tracing app may have left the door unlocked to a privacy breach. Sam Morris/Getty Images

When Google and Apple introduced their COVID-19 contact tracing framework in April 2020, the companies aimed to reassure people worried about sharing private health information with major corporations.

Google and Apple provided assurances that the data generated through the apps—people’s movements, who they might have come in contact with, and whether they reported testing positive for COVID-19—would be anonymized and would never be shared with anyone other than public health agencies.

“Our goal is to empower [public health agencies] with another tool to help combat the virus while protecting user privacy,” Google CEO Sundar Pichai wrote in a tweet last May, when the framework became publicly available.

Apple CEO Tim Cook provided similar assurances.

Since then, millions of people have downloaded contact tracing apps developed through Apple’s and Google’s framework: The U.K.’s National Health Services’ app has at least 16 million users, while Canada’s Digital Service COVID Alert app boasted more than six million downloads in January, and Virginia’s Department of Health noted more than two million residents were using its COVIDWISE app.

California governor Gavin Newsom endorsed his state’s version of the app, calling it “100% private & secure” in a tweet last December.

But The Markup has learned that not only does the Android version of the contact tracing tool contain a privacy flaw, but when researchers from the privacy analysis firm AppCensus alerted Google to the problem back in February of this year, Google failed to change it. AppCensus was testing the system as part of a contract with the Department of Homeland Security. The company found no similar issues with the iPhone version of the framework.

“This fix is a one-line thing where you remove a line that logs sensitive information to the system log. It doesn’t impact the program, it doesn’t change how it works, ” said Joel Reardon, co-founder and forensics lead of AppCensus. “It’s such an obvious fix, and I was flabbergasted that it wasn’t seen as that.”

“We were notified of an issue where the Bluetooth identifiers were temporarily accessible to specific system level applications for debugging purposes, and we immediately started rolling out a fix to address this,” Google spokesperson José Castañeda said in an emailed statement to The Markup.

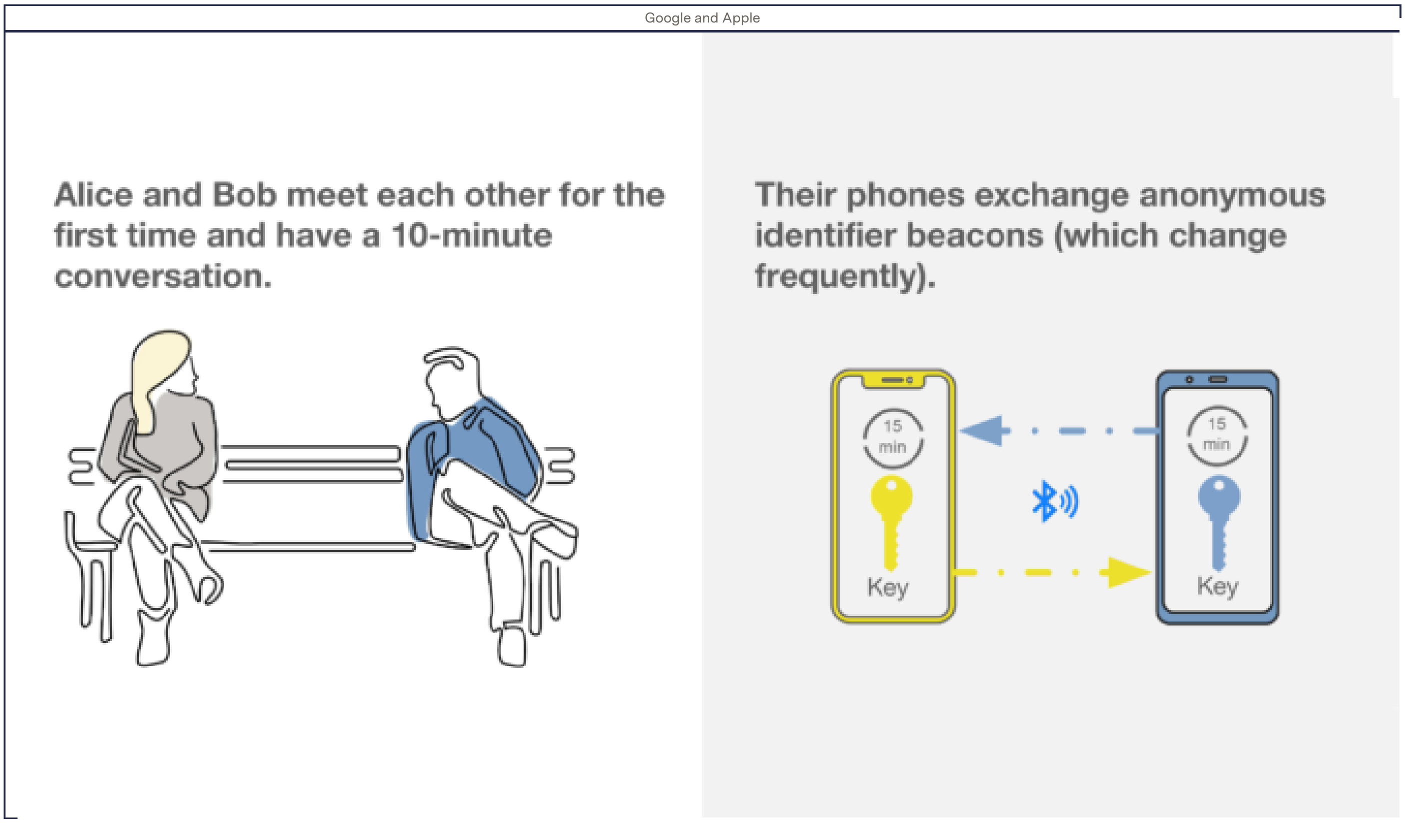
Serge Egelman, AppCensus’s co-founder and chief technology officer, however, said that Google had repeatedly dismissed the firm’s concerns about the bug until The Markup contacted Google for comment on the issue late last week.

Asked if the vulnerability has been eliminated, Castañeda said the “roll out of this update to Android devices began several weeks ago and will be complete in the coming days.”

The issue, Reardon said, is that hundreds of preinstalled apps like Samsung Browser and Motorola's MotoCare on Android devices have access to potentially sensitive information that the contact tracing apps store in system logs—a byproduct of how the preinstalled apps receive information about user analytics and crash reports.

The contact tracing tool works by exchanging anonymized Bluetooth signals with other phones that have the contact tracing app. Those signals are changed every 15 minutes to make it harder to identify someone and are created from a key that changes every 24 hours.

Google and Apple


Alice and Bob meet each other for the first time and have a 10-minute conversation.
Their phones exchange anonymous identifier beacons (which change frequently).
15 min
Key
15 min
Key

Google and Apple explained how "rolling proximity identifiers" are exchanged.

The signals that a phone's contact tracing data generates and receives are saved into an Android device's system logs. Studies have found that more than 400 preinstalled apps on phones built by Samsung, Motorola, Huawei, and other companies have permission to read system logs for crash reports and analytic purposes.

In the case of contact tracing apps, Reardon found that the system logs included data on whether a person was in contact with someone who tested positive for COVID-19 and could contain identifying information such as a device's name, MAC address, and advertising ID from other apps. In theory, that information could be swept up by preinstalled apps and sent back to their company's servers. He has not found that any apps have actually gathered that data, but there's nothing preventing them from doing so.

"What Google is saying is that these logs never leave the device," Reardon said. "They can't make that claim—they don't know if any of these apps are collecting the system logs."

"These Bluetooth identifiers do not reveal a user's location or provide any other identifying information and we have no indication that they were used in any way—nor that any app was even aware of this," Castañeda, the Google spokesperson, said in the email to The Markup.

Google has made several public promises that all contact tracing data would be processed on a user's phone and not sent to any servers. While the apps are exchanging anonymized Bluetooth signals, the only time any data would be sent to an outside entity would be if a user identified themself as testing positive for COVID-19 and chose to share that information with public health authorities.

When Google and Apple first released the tool, they promised "the list of people you've been in contact with doesn't leave your phone unless you choose to share it" during a press briefing.

At the International Association of Privacy Professionals' keynote event last July, Google's and Apple's chief privacy officers highlighted that storing and processing the data only on devices instead of servers protected their users' privacy.

"We felt strongly that all this exposure notification information being done on [the] device and that processing being done under the strict controls of the user was an essential design feature to optimize for the privacy of the system," Keith Enright, Google's chief privacy officer, said at the panel.

Connecticut's privacy policy for the state's contact tracing app also notes that data is stored only on a user's device and isn't shared unless a person has a positive COVID-19 diagnosis and chooses to share that information. The state's app is based on Google's and Apple's exposure notification framework.

"These data are stored only on the user's device and are never shared unless and until the user has a positive COVID-19 diagnosis and elects to share this information within the system," the policy states.

Reardon first reached out to Google about the issue on Feb. 19, filing a report to Google's bug bounty program.

Google has a program in which it pays researchers for finding security issues with its services but only if the company considers it a serious enough flaw. The team didn't believe Reardon's findings met its standards, according to emails provided to The Markup by AppCensus.

On March 12, Reardon received an email from "Enzo, Google Security Team" that said, "This might not be severe enough to qualify for a reward, though the panel will take a look at the next meeting and we'll update you once we've got more information. All you need to do now is wait. If you don't hear back from us in 2-3 weeks or have additional information about the vulnerability, let us know."

Four days later, Reardon received an automated email from Google telling him it had confirmed that the flaw wasn't enough to warrant a payout, and that the security team would "decide whether they want to make a change or not."

He said he hasn't heard from the company since.

Reardon also reached out to Giles Hogben, Android's director of privacy engineering, on Feb. 19. In an email, Hogben noted, in response to Reardon's concerns, that the system logs could only be accessed by certain apps.

"[System logs] have not been readable by unprivileged apps (only with READ_LOGS privileged permission) since way before Android 11 (can check exactly when but I think back as far as 4)," Hogben said in his Feb. 25 reply.

Reardon, however, said hundreds of preinstalled apps can still read those system logs. "They're actually collecting information that would be devastating to the privacy of people who use contact tracing," he said.