Exposure Notification

Frequently Asked Questions

Preliminary — Subject to Modification and Extension

May 2020

v1.1

Overview

On April 10, 2020 Google and Apple announced a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of COVID-19 through contact tracing, with user privacy and security core to the design. Since that announcement, stakeholders including developers, consumers, health agencies and governments have reached out with questions. This document serves to address these questions and provide more clarity and transparency in the process.

1. What is conventional contact tracing and how does it work?

Conventional contact tracing is a technique used by public health authorities to measure and slow the spread of infectious diseases. It requires manually gathering information from infected individuals about the people they've previously been in contact with. These people can then be notified by public health authorities to take appropriate safety measures, such as undertaking self-quarantine and getting tested to break the chain of transmission. While this process will continue to be important to contact tracing efforts, we believe the system we developed can alleviate some of the challenges with this process. First there is a significant organizational burden from a manual process, as many public health workers are needed to perform these tasks. Second, the process can be a slow as it requires finding and interviewing infected individuals and then reaching out and talking to their high risk contacts - all of whom may not be able to remember or know all of the people that they came in contact with in the past days to weeks.

2. Can contact tracing help with slowing COVID-19?

Yes. Contact tracing has been used to slow down transmission for many infectious diseases in the past. Each contact tracing effort is unique in some ways as they manage the specific challenges of individual infectious diseases. Governments, public health authorities, and NGOs around the world are starting to deploy contact tracing as a valuable tool for managing the COVID-19 pandemic.

3. How can technology augment conventional contact tracing?

Technology can play an important role in those efforts. Mobile devices can be used in an automated and scalable way to help determine who has been exposed to a person that later reports a positive diagnosis of COVID-19. For example, they can be used to send a rapid notification to the exposed person with instructions on next steps. These notifications may be beneficial by alerting an exposed individual faster than they would be notified via conventional contact tracing. They will enable public health authorities to contact and provide guidance to the individual and, where appropriate, include them in conventional contact tracing efforts. Using digital exposure notifications is new and individual health authorities are determining how they best fit into their own public health systems.

4. What have Apple and Google announced as a technology solution and how does it work?

On April 10, 2020, Google and Apple announced a two-phase exposure notification solution that uses Bluetooth technology on mobile devices to aid in contact tracing efforts.

Both phases of the solution harness the power of Bluetooth technology to aid in exposure notification. Once enabled, users' devices will regularly send out a beacon via Bluetooth that includes a random Bluetooth identifier — basically, a string of random numbers that aren't tied to a user's identity and change every 10-20 minutes for additional protection. Other phones will be listening for these beacons and broadcasting theirs as well. When each phone receives another beacon, it will record and securely store that beacon on the device.

At least once per day, the system will download a list of the keys for the beacons that have been verified as belonging to people confirmed as positive for COVID-19. Each device will check the list of beacons it has recorded against the list downloaded from the server. If there is a match between the beacons stored on the device and the positive diagnosis list, the user may be notified and advised on steps to take next.

To power this solution in the first phase, both companies will release application programming interfaces (APIs) that allow contact tracing apps from public health authorities to work across Android and iOS devices, while maintaining user privacy. These apps from public health authorities will be available for users to download via their respective app stores. Once the app is launched, the user will then need to consent to the terms and conditions before the program is active. The companies plan to make these APIs available in May.

In the second phase, available in the coming months, this capability will be introduced at the operating system level to help ensure broad adoption, which is vital to the success of contact tracing. After the operating system update is installed and the user has opted in, the system will send out and listen for the Bluetooth beacons as in the first phase, but without requiring an app to be installed. If a match is detected the user will be notified, and if the user has not already downloaded an official public health authority app they will be prompted to download an official app and advised on next steps. Only public health authorities will have access to this technology and their apps must meet specific criteria around privacy, security, and data control.

If at some point a user is positively diagnosed with COVID-19, he or she can work with the health authority to report that diagnosis within the app, and with their consent their beacons will then added to the positive diagnosis list. User identity will not be shared with other users, Apple and Google as part of this process.
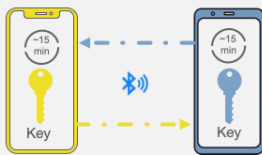
Alice and Bob don't know each other, but have a lengthy conversation sitting a few feet apart
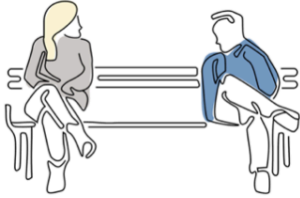
Bob is positively diagnosed for COVID-19 and enters the test result in an app from his public health authority

A few days later…

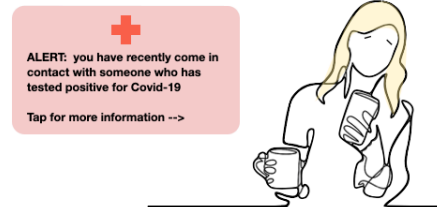Their phones exchange beacons with random Bluetooth identifiers (which change frequently)

With Bob's consent, his phone uploads the last 14 days of keys for his Bluetooth beacons to the server

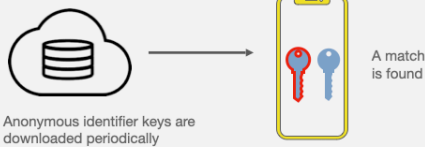Apps can only get more information via user consent

Positive Test
Submit

~14 day temporary store

Key

Key

🍎 | Google

Alice continues her day unaware she had been near a potentially contagious person

Alice sees a notification on her phone

ALERT: you have recently come in contact with someone who has tested positive for Covid-19

Tap for more information -->

Sometime later…

Alice's phone periodically downloads the Bluetooth beacon keys of everyone who has tested positive for COVID-19 in her region. A match is found with Bob's random Bluetooth identifiers.

Alice's phone receives a notification with information about what to do next.

A match is found

Anonymous identifier keys are downloaded periodically

Additional information is provided by the health authority app

🍎 | Google

5. How will the system protect user privacy and security?

Google and Apple put user privacy at the forefront of this exposure notification technology's design and have established strict guidelines to ensure that privacy is safeguarded:

- Each user will have to make an explicit choice to turn on the technology. It can also be turned off by the user at any time.

- This system does not collect location data from your device, and does not share the identities of other users to each other, Google or Apple. The user controls all data they want to share, and the decision to share it.

- Random Bluetooth identifiers rotate every 10-20 minutes, to help prevent tracking.

- Exposure notification is only done on device and under the user's control. In addition people who test positive are not identified by the system to other users, or to Apple or Google.

- The system is only used for contact tracing by public health authorities apps.

- Google and Apple will disable the exposure notification system on a regional basis when it is no longer needed.

   a. **Can I turn it off?**

Yes. The choice to use this technology rests with the user, and he or she can turn it off at any time by uninstalling the contact tracing application or turning off exposure notification in Settings.

6. Will governments have access to the information facilitated by this technology?

The goal of this project is to assist public health authorities in their efforts to fight COVID-19 by enabling exposure notification in a privacy-preserving manner and the system is designed so that the identities of the people a device comes in contact with are protected.

Access to the technology will be granted only to public health authorities. Their apps must meet specific criteria around privacy, security, and data control. The public health authority app 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 system was also designed so that Apple and Google do not have access to information related to any specific individual.

7. Where is the data stored and who has access to it?

If a user decides to participate, exposure notification data will be stored and processed on device. Other than the random Bluetooth identifiers that are broadcast, no data will be shared by the system with public health authority apps unless one of the following two scenarios takes place:

- **If a user chooses to report a positive diagnosis of COVID-19 to their contact tracing app**, the user's most recent keys to their Bluetooth beacons will be added to the positive diagnosis list shared by the public health authority so that other users who came in contact with those beacons can be alerted.

- **If a user is notified through their app that they have come into contact with an individual who is positive for COVID-19** then the system will share the day the contact

occurred, how long it lasted and the Bluetooth signal strength of that contact. Any other information about the contact will not be shared.

In keeping with our privacy guidelines, Apple and Google will not receive identifying information about the user, location data, or information about any other devices the user has been in proximity of.

8. Will my data be monetized by Google or Apple?

No, there will be no monetization from this project by Apple or Google. Consistent with well-established privacy principles, both companies are minimizing data used by the system and relying on users' devices to process information.

9. Who will create the apps and where do I find them?

Public health authorities will update or create apps which users may install if they choose to participate. Google and Apple will make available, as normal, the public health authority apps for each region in the Play Store and App Store.

10. How will apps get approval to use this system?

Apps will receive approval based on a specific set of criteria designed to ensure they are only administered in conjunction with public health authorities, meet our privacy requirements, and protect user data.

The criteria are detailed separately in agreements that developers enter into to use the API, and are organized around the principles of functionality and user privacy. There will be restrictions on the data that apps can collect when using the API, including not being able to request access to location services, and restrictions on how data can be used.

11. What public health authority can users contact about the app for their region?

Google and Apple are currently in discussion with various public health authorities globally to provide them with this technology. Both companies will highlight public health authority apps that have been given access to this technology when they are available.

12. How do users report themselves as positive for COVID-19?

The mechanism for allowing users to report themselves as positive will be determined by the relevant public health authority and may vary across regions. For example, some public health authorities may allow users to verify a test result using a pin code, while others may provide different mechanisms for verification.

13. How does the system know when I have been exposed?

The public health authority will define the way in which the app determines if someone has been exposed. To support this the system provides apps with both an estimate of time the user

has been in contact with someone who has been diagnosed as positive for COVID-19 and the approximate distance between the users. Public health authorities will set a minimum threshold for time spent together, such that a user needs to be within Bluetooth range for at least 5 minutes to register a match. If the contact is longer than 5 minutes, the system will report time in increments of 5 minutes up to a maximum of 30 minutes to ensure privacy.

To approximate distance, the system compares the Bluetooth signal strength between the two devices in contact. The closer the devices are, the higher the signal strength recorded. This signal strength can vary significantly based on factors like how the device is being held and as such this only provides an estimate of distance.

Conclusion

There are many responses to COVID-19 including protecting the vulnerable, building new protocols for daily life to reduce transmission, and containing inevitable local outbreaks of coronavirus. Testing and contact tracing will be critical to this last strategy, especially, in light of the high transmission rate of COVID-19 and exposure notification can be a key addition to the toolbox of public health authorities. As the response to the pandemic evolves, technological solutions will need to continue to adapt as well so the efforts of public health authorities can be amplified.

The technical details of the system are described in more detail in the technical white papers available here:

https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/

https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/