GuideSafe Contact Tracing Privacy Information

There has been a lack of details and many concerns over the UA System's promotion of the GuideSafe COVID-19 contact tracing "app", so I wanted to shed some light on what the app is actually doing. As of Apple iOS 13.5 (May 22, 2020) and the May 2020 update to Android's Google Play Services, Google and Apple have been jointly collecting (within your device) COVID-19 exposure information on your Google/Apple updated device(s). More information can be found here:

https://www.google.com/covid19/exposurenotifications/

To view these settings on your device(s):

Android: open Settings, then tap Google and COVID-19 Exposure Notifications

Apple: open Settings, select Privacy, Health, and COVID-19 Exposure Logging

The GuideSafe app is a subscriber of the logs kept by the Google/Apple operating systems. It is one of the first contact tracing apps to use the infrastructure, but many more are in the works, and users can be part of multiple contact tracing systems at the same time. With user permission, the app reads the logs and sends the logs to servers. In the case of GuideSafe, the server is denoted as belonging to ADPH. The server then checks its master list of known infections and sends back the date and time of possible infection exposure.

How does this happen?

When your device is within Bluetooth range (up to 100ft) of another device, data/device information exchanges occur. This is a function of Bluetooth and existed long before COVID-19. With the Google/Apple update, your phone sends IDs that are cryptographic "hashes", that are one-way calculations that cannot be reversed back to a person or device. These IDs often change, and the master key from which they are created also changes daily to further ensure privacy. Since Bluetooth operates at a long distance, even through walls, the signal level of the Bluetooth is used to guess at the distance from another device. This distance, along with the time duration that your device "sees" the other device is used to create a measure of exposure. This data is then logged to your device.

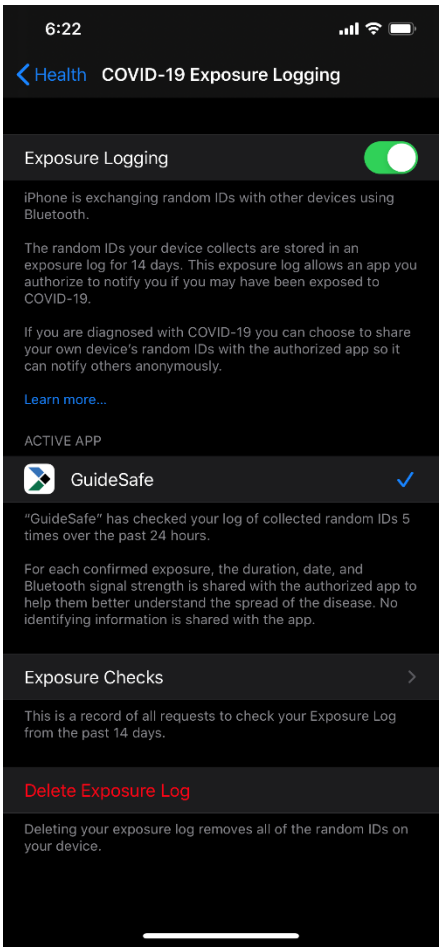

Figure 1 - iOS COVID-19 Tracking with GuideSafe

What leaves my device, and what comes back?

The log of exposure IDs and dates/times, which are non-identifiable, are sent to a central server for "contact tracing" if an app such as GuideSafe is installed on your device. GuideSafe sends data to what is denoted in the logs as an ADPH server. Without GuideSafe or another contact tracing app, the data remains dormant on your device. The contact tracing app and back-end server "connect the dots" between who you have been in contact with and who have reported positive to the central authority. The information sent to ADPH is the list of IDs that you have come in contact with over the past rolling 14-day period. The ADPH server takes your list and compares your list to data that it has received from other participating devices. If ADPH has received a positive test from another device and that device is on your list, you receive an indication of possible exposure with a date and time.

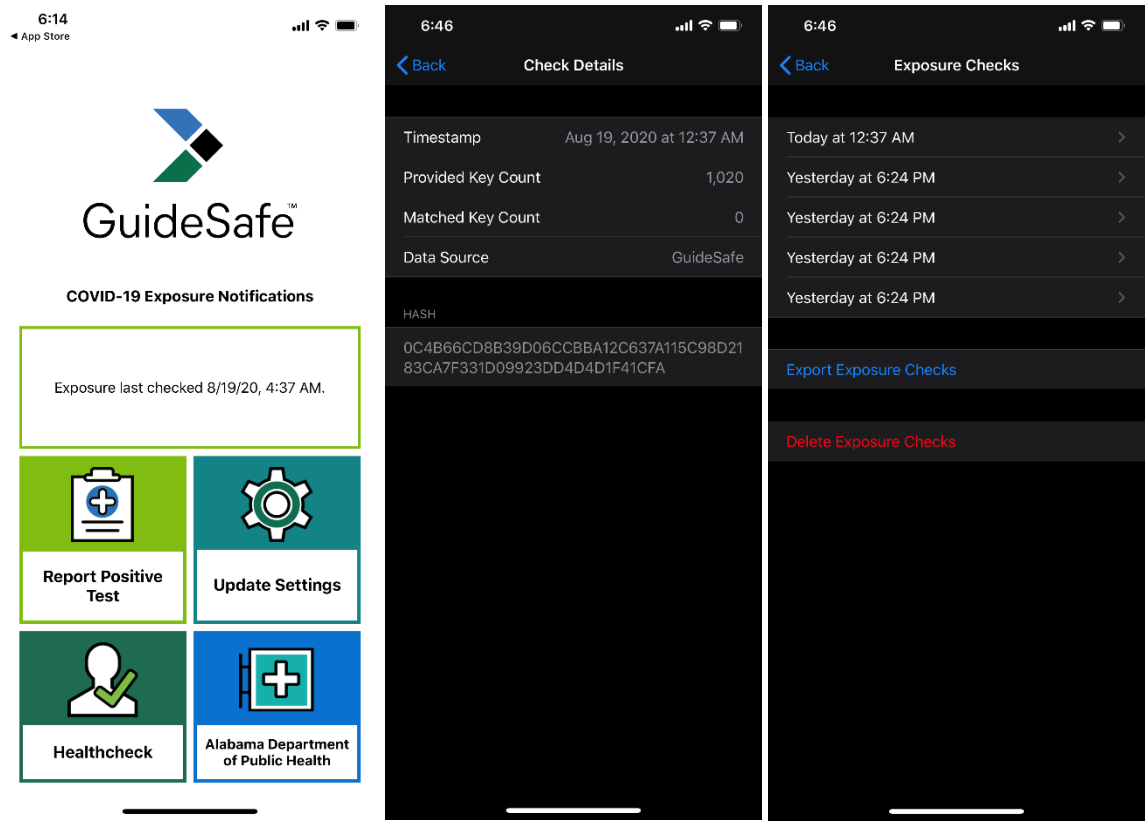

Figure 2 - Contact Tracing Logs

How are exposures collected?

Within the GuideSafe app, there is a "Report Positive Test" button. Clicking this button prompts the user for their phone number so that they can receive a security verification code. This is, so the system is not flooded with fake test results. The operating system/phone then asks the user if it is ok to share the stored list of its past 14 days of identifiers with the central server (ADPH for GuideSafe). If the user accepts, then its identifiers are sent to the central server. That list is the core of how other devices are made aware of exposure as the server matches up identifiers of devices that a user has come in contact with to the list of identifiers provided from a person that has tested positive.

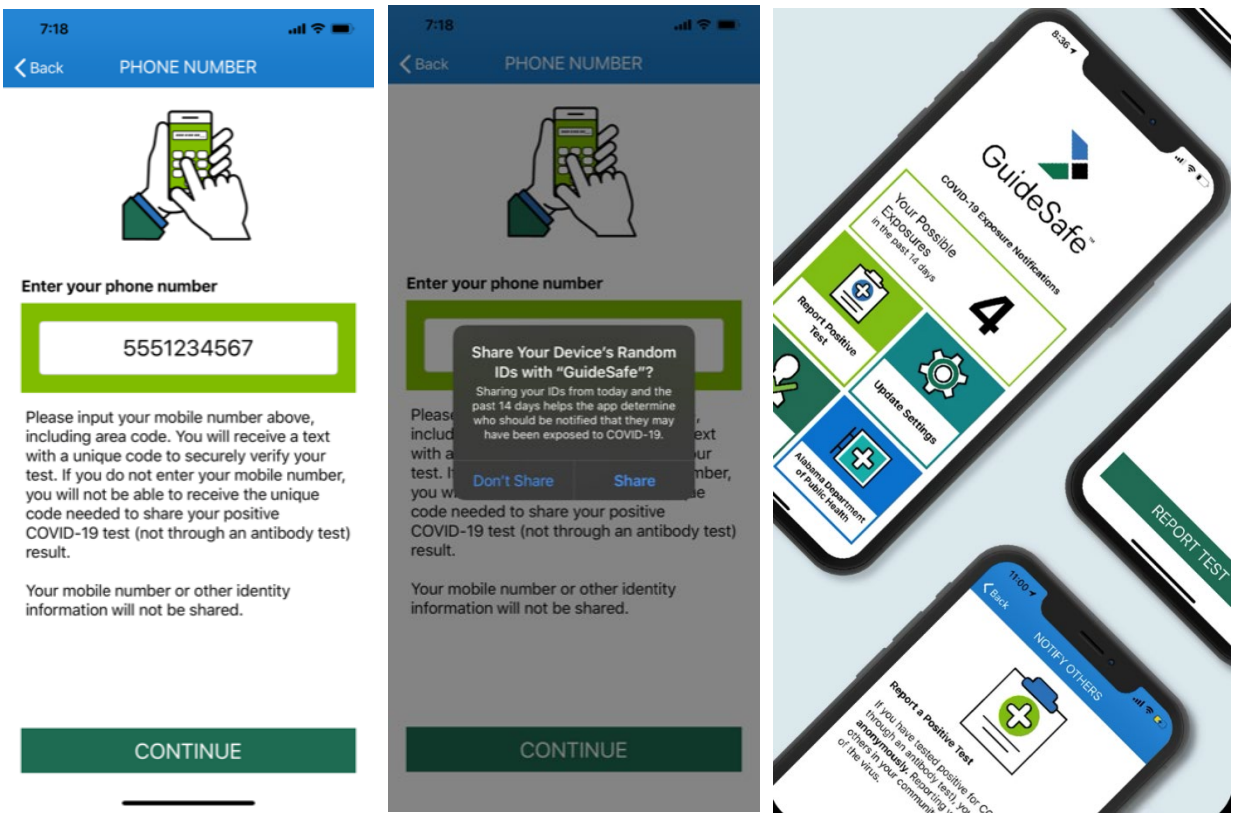

Figure 3 - Positive Case Submission

Are there security concerns?

This is a tough question as with technology, there are always security concerns. The processes for exchanging IDs/data were done by Google/Apple, so that definitely increases the odds that they were done correctly. However, it would be fairly trivial to design another app that tracks Bluetooth identifiers and phone names and then reads the log on a device. This app could then provide a list of likely phones that might be the match to the exposure notification one received. This is an extreme example, and other side-channel types of "attacks" may be possible as well.

Irrespective of these concerns, no location information is being shared outside of your device to UA, ADPH, or other entities in terms of COVID tracking. Your positive test results are sent to ADPH, but it is unclear at this point where the ADPH server resides and who all has access to the data. Overall though, the app and infrastructure appear to be exchanging information in a secure and safe manner.

For more information on GuideSafe and the Apple/Google contact tracing, see these links:

https://www.guidesafe.org/

https://www.wired.com/story/covid-19-contact-tracing-apple-google/