

Apple rejects flawed claims about its contact tracing tech

Apple has been forced to reject damaging claims against its contact tracing tech now circulating on Facebook.

Even as we consider revelations Facebook shelved internal research suggesting its algorithms generate divisiveness, Apple has been forced to reject damaging claims against its contact tracing tech currently spreading on Facebook.

Exposure Notification is not spying on you

Numerous hysterical myths concerning the Apple/Google contact tracing technology are being circulated on Facebook. A series of posts claim the Exposure Notification feature inside iOS 13.5 will allow authorities to track people's locations and monitor who they meet – which is precisely what it tries not to do.

This is not correct.

[Keep up on the latest thought leadership, insights, how-to, and analysis on IT through Computerworld's newsletters.]

The solution requires individuals use a government-approved app and that they consent to sharing any information. Not only this, but both Apple and Google have barred governments from harvesting GPS data or requiring users to share personal information when using the app.

An Apple spokesperson told Reuters:

“You will still need to download an app from a public health agency to use the Exposure

Notifications feature.”

How it works

In order to work, the solution relies on random Bluetooth identifiers shared between devices. This information forms a record of proximity but does not include location data.

[Take this mobile device management course from PluralSight and learn how to secure devices in your company without degrading the user experience.]

When they announced their work, Apple and Google promised that any apps using the technology “must require users to consent before ☐ sharing a positive test result, and the ☐ ‘keys’ ☐ associated with their devices, with ☐ the public health authority.” Users should also be able to turn off exposure notifications at any time.

The tech firms are attempting to create a contact tracing solution that gathers as little personal information as possible, and have previously promised to delete the feature once the current crisis has passed.

The intention of the tech is that government or health authorities can use the API to build apps with which to monitor the disease outbreak.

What is contact tracing?

Contact tracing is seen as a way to help control the pandemic. The information should warn people when they have been exposed to the diseases.

This could enable life to return to something a little more like business as usual, while also saving lives – though the efficiency is limited if people refuse to use the apps.

The tech-based solution won't be the only tool used for this: Many governments are hiring tens of thousands of human contact tracers to interview COVID-19 sufferers in order to find out who they have interacted with.

Apple and Google continue development

Apple and Google both released APIs for their technology earlier this month. These are designed to make it possible for both Android and iOS devices to work together for contact tracing using officially sanctioned government apps.

The two companies are also developing a broader Bluetooth-based contact tracing platform by building this functionality into the underlying platforms, they said in April.

"This is a more robust solution than an API and would allow more individuals to participate, if they choose to opt in, as well as enable interaction with a broader ecosystem of apps and government health authorities," the companies explained at that time.

"Privacy, transparency, and consent are of utmost importance in this effort, and we look forward to building this functionality in consultation with interested stakeholders."

Who is using these apps ?

Apple and Google have said 23 countries and several U.S. states have requested access to its APIs. The first app to make use of the Apple/Google API has appeared in Switzerland, with a Latvian initiative not far behind.

There are some governments who want to gather all the information for analysis on servers they

control, but the Apple/Google model does not enable this; instead, analysis takes place on the device.

The idea is that by retaining control of data on user devices, privacy is maintained.

Those countries attempting to gather this data in a far less private, centralized fashion are having problems creating solutions that actually work.

One app tested in the UK is glitchy, drains batteries and doesn't work well between platforms, among other problems. That's a shame, given that it now has a higher death rate per million than any other country in the world, and could probably use an effective solution.

Please follow me on Twitter, or join me in the AppleHolic's bar & grill and Apple Discussions groups on MeWe.