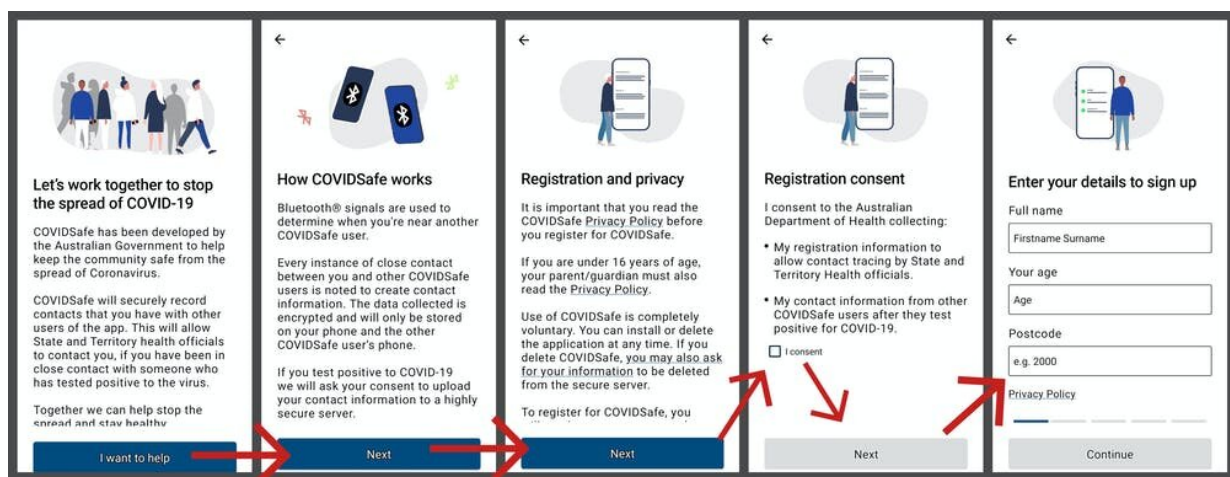# COVIDSafe tracking app reviewed: the government delivers on data security, but other issues remain

April 27 2020, by Mahmoud Elkhodr

These screens that show up upon app installation explain the app's functions and guide users through registration.

About 1.13 million people had downloaded the federal government's COVIDSafe app by 6am today, just 12 hours after its release last night, said Health Minister Greg Hunt. The government is hoping at least 40% of the population will make use of the app, designed to help reduce the spread of the coronavirus disease.

Previously dubbed TraceTogether – in line with a similar app rolled out

in Singapore—the [coronavirus](#) contact tracing app has been an ongoing [cause of contention](#) among the public. Many people have voiced concerns of an erosion of privacy, and potential misuse of citizen data by the government.

But how does COVIDSafe work? And to what extent has the app addressed our privacy concerns?

Getting started

The app's landing page outlines its purpose: to help Australian health authorities trace and prevent COVID-19's spread by contacting people who may have been in proximity (to a distance of [about 1.5 metres](#)) with a confirmed case, for 15 minutes or more.

The second screen explains how Bluetooth technology is used to record users' contact with other app users. This screen says collected data is encrypted and can't be accessed by other apps or users without a decryption mechanism. It also says the data is stored locally on users' phones and isn't sent to the government (remote server storage).

In subsequent screens, the app links to its [privacy policy](#), seeks user consent to retrieve registration details, and lets users register by entering their name, age range, postcode and mobile number.

This is followed by a declaration page where the user must give consent to enable Bluetooth, "location permissions" and "battery optimiser".

4⁺ᵍ .ııll 🗐 ☒   ⋯ ⑨ 96% 🔋10:30

←

App permissions

COVIDSafe needs Bluetooth® and
notifications enabled to work.

Select 'Proceed' to enable:

1. Bluetooth®

2. Location Permissions

3. Battery Optimiser

Android needs Location
Permissions for Bluetooth® to

Proceed

COVIDSafe requires certain permissions to run.

In regards to enabling location permissions, it's important to note this isn't the same as turning on location services. Location permissions must be enabled for COVIDSafe to access Bluetooth on Android and Apple devices. And access to your phone's battery optimiser is required keep the app running in the background.

Once the user is registered, a notification should confirm the app is up and running.

Importantly, COVIDSafe doesn't have an option for users to exit or "log-off".

Currently, the only way to stop the app is to uninstall it, or turn off Bluetooth. The app's reliance on prolonged Bluetooth usage also has users worried it might quickly drain their phone batteries.

Preliminary tests

Upon preliminary testing of the app, it seems the federal government has delivered on its promises surrounding data security.

Tests run for one hour showed the app didn't transmit data to any external or remote server, and the only external communication made was a "handshake" to a remote server. This is simply a way of establishing a secure communication.

Additional tests should be carried out on this front.
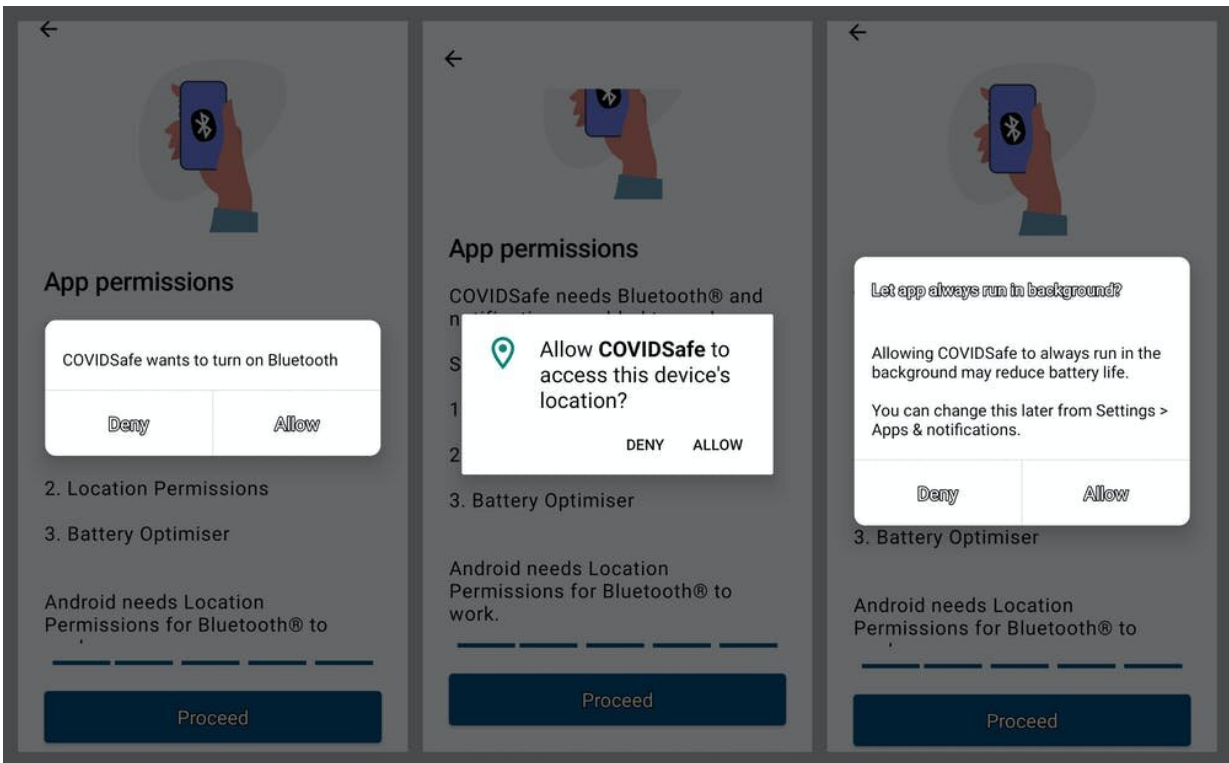
Users will have to manually grant some permissions.

Issues for iPhone users

[According to reports](#), if COVIDSafe is being used on an iPhone in low-power mode, this may impact the app's ability to track contacts.

Also, iPhone users must have the app open (in the foreground) for Bluetooth functionality to work. The federal government plans to fix this hitch "in a few weeks", according to *The Guardian*.

This complication may be because Apple's operating system generally doesn't allow apps to run Bluetooth-related tasks, or perform Bluetooth-related events [unless running in the foreground](#).

Source code

"Source code" is the term used to describe the set of instructions written during the development of a program. These instructions are understandable to other programmers.

In a privacy impact assessment response from the Department of Health, the federal government said it would make COVIDSafe's source code publicly available, "subject to consultation with" the Australian Cyber Security Centre. It's unclear exactly when or how much of the source code will be released.

Making the app's source code publicly available, or making it "open source", would allow experts to examine the code to evaluate security risks (and potentially help fix them). For example, experts could determine whether the app collects any personal user information without user consent. This would ensure COVIDSafe's transparency and enable auditing of the app.
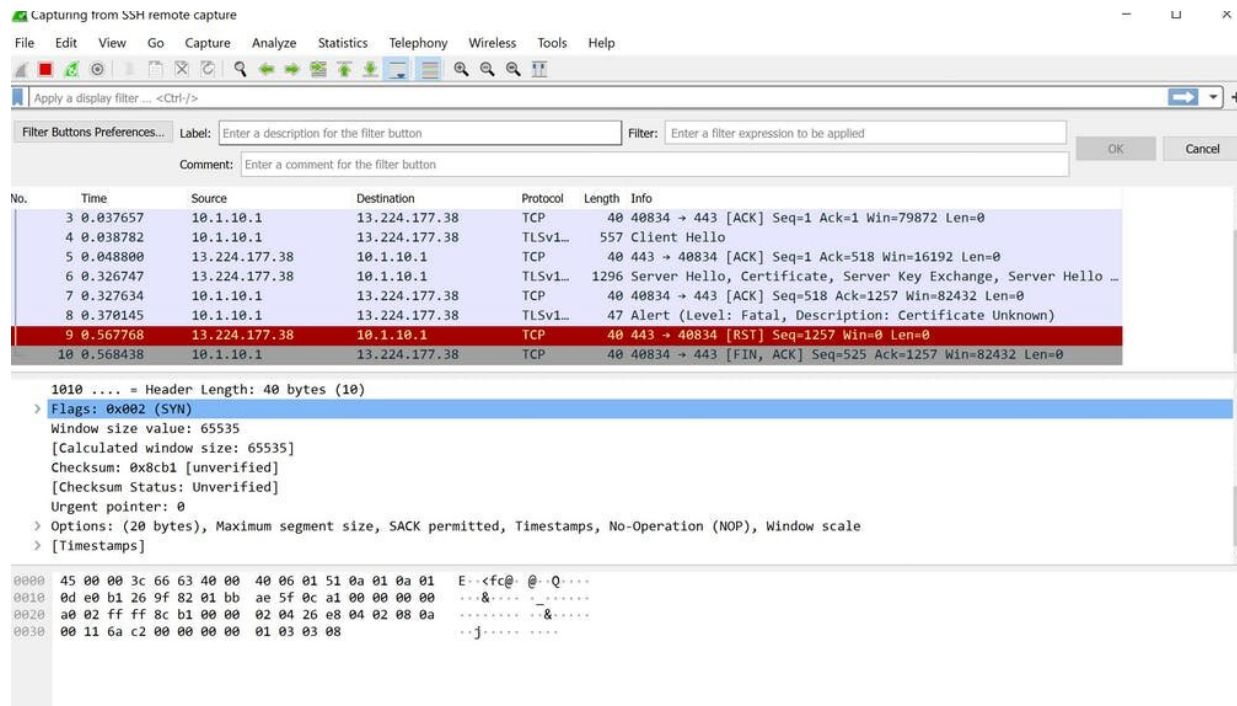
This screenshot shows test results run via the Wireshark software to determine whether data from COVIDSafe was being transmitted to external servers.

Releasing the [source code](#) isn't only important for transparency, but also for understanding the app's functionality.

Some COVIDSafe users [reported](#) the app wouldn't accept their mobile number until they turned off wifi and used their mobile network (4G) instead. Until the app is made open source, it's difficult to say exactly why this happens.

Civic duty

Overall, it seems COVIDSafe is a promising start to the national effort to ease lockdown restrictions, a luxury [already afforded to some states](#) including Queensland.

Questions have been raised around whether the app will later be made compulsory to download, to reach the 40% uptake target. But current growth in download numbers suggests such enforcement may not be necessary as more people rise up to their "civic duty".

That said, only time will reveal the extent to which Australians embrace this new contact tracing technology.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation