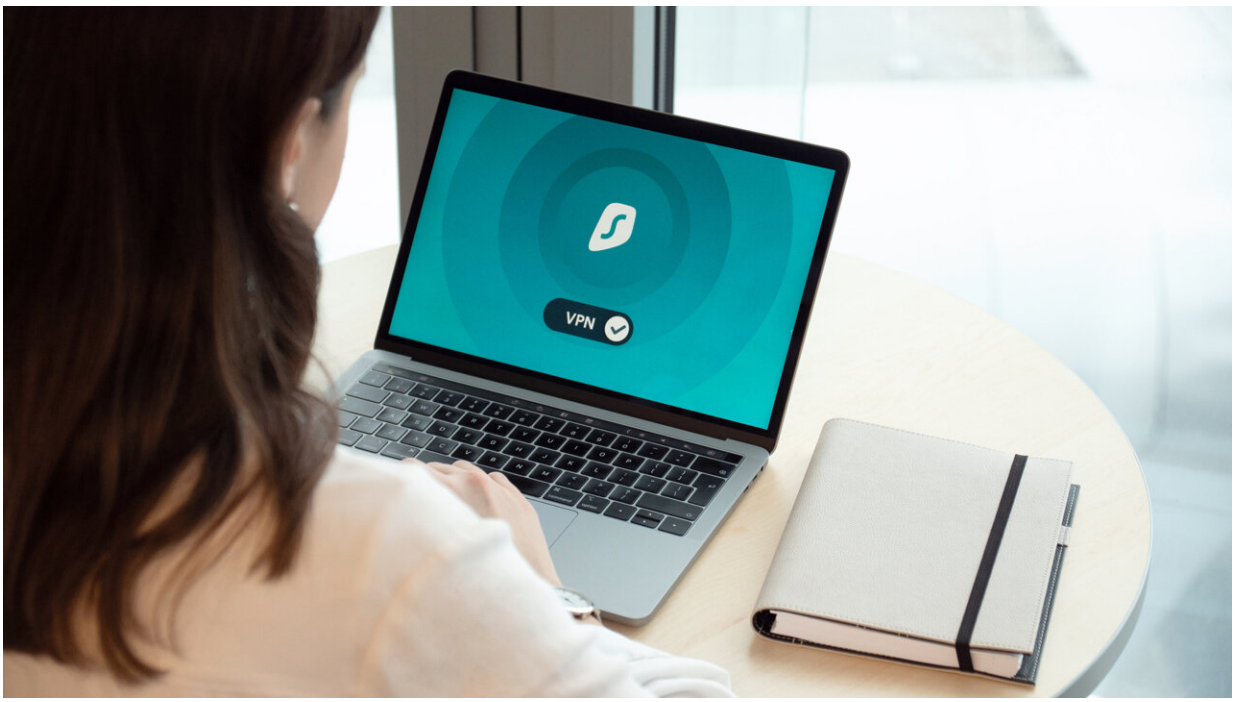
How safe is COVIDSafe? What you should know about the app's issues, and Bluetooth-related risks

May 7 2020, by James Jin Kang and Paul Haskell-Dowland



Credit: Dan Nelson from Pexels

The Australian government's COVIDSafe app has been up and running for almost a fortnight, with more than five million downloads.

Unfortunately, since its release many users—particularly those with

iPhones—have been in the dark about how well the app works.

Digital Transformation Agency head Randall Brugeaud has now admitted the app's effectiveness on iPhones "deteriorates and the quality of the connection is not as good" when the phone is locked, and the app is running in the background.

There has also been confusion regarding where user data is sent, how it's stored, and who can access it.

Conflicts with other apps

Using Bluetooth, COVIDSafe collects anonymous IDs from others who are also using the app, assuming you come into range with them (and their smartphone) for a period of at least 15 minutes.

Bluetooth must be kept on at all times (or at least turned on when leaving home). But this setting is specifically advised against by the Office of the Australian Information Commissioner.

It's likely COVIDSafe isn't the only app that uses Bluetooth on your phone. So once you've enabled Bluetooth, other apps may start using it and collecting information without your knowledge.

Bluetooth is also energy-intensive, and can quickly drain phone batteries, especially if more than one app is using it. For this reason, some may be reluctant to opt in.

There have also been reports of conflicts with specialized medical devices. Diabetes Australia has received reports of users encountering problems using Bluetooth-enabled glucose monitors at the same time as the COVIDSafe app.

If this happens, the current advice from Diabetes Australia is to uninstall COVIDSafe until a solution is found.

Bluetooth can still track your location

Many apps require a Bluetooth connection and can track your location without actually using GPS.

Bluetooth "beacons" are progressively being deployed in public spaces—with one example in Melbourne supporting visually impaired shoppers. Some apps can use these to log locations you have visited or passed through. They can then transfer this information to their servers, often for marketing purposes.

To avoid apps using Bluetooth without your knowledge, you should deny Bluetooth permission for all apps in your phone's settings, and then grant permissions individually.

If privacy is a priority, you should also read the privacy policy of all apps you download, so you know how they collect and use your information.

Issues with iPhones

The iPhone operating system (iOS), depending on the version, doesn't allow COVIDSafe to work properly in the background. The only solution is to leave the app running in the foreground. And if your iPhone is locked, COVIDSafe may not be recording all the necessary data.

You can change your settings to stop your iPhone going into sleep mode. But this again will drain your battery more rapidly.

Brugeaud said older models of iPhones would also be less capable of

picking up Bluetooth signals via the app.

It's expected these issues will be fixed following the integration of contact tracing technology developed by Google and Apple, which Brugeaud said would be done within the next few weeks.

Vulnerabilities to data interception

If a user tests positive for COVID-19 and consents to their data being uploaded, the information is then held by the federal government on an Amazon Web Services server in Australia.

Data from the app is stored on a user's device and transmitted in an encrypted form to the server. Although it's technically possible to intercept such communications, the data would still be encrypted and therefore offer little value to an attacker.

The government has said the data won't be moved offshore or made accessible to US law enforcement. But various entities, including Australia's Law Council, have said the privacy implications remain murky.

That said, it's reassuring the Amazon data center (based in Sydney) has achieved a very high level of security as verified by the Australian Cyber Security Centre.

Can the federal government access the data?

The federal government has said the app's data will only be made available to state and territory health officials. This has been confirmed in a determination under the Biosecurity Act and is due to be implemented in law.

Federal health minister Greg Hunt said: "Not even a court order during an investigation of an alleged crime would be allowed to be used [to access the data]."

Although the determination and proposed legislation clearly define the *who* and *how* of access to COVIDSafe data, past history indicates the government may not be best placed to look after our data.

It seems the government has gone to great lengths to promote the security and privacy of COVIDSafe. However, the government commissioned the development of the app, so *someone* will have the means to obtain the information stored within the system—the "keys" to the vault.

If the government did covertly obtain access to the data, it's unlikely we would find out.

And while contact information stored on user devices is deleted on a 21-day rolling basis, the Department of Health has said data sent to Amazon's server will "be destroyed at the end of the pandemic." It's unclear how such a date would be determined.

Ultimately, it comes down to trust—something which seems to be in short supply.

Provided by The Conversation

https://techxplore.com/news/2020-05-safe-covidsafe-app-issues-bluetooth-related.html