COVIDSAFE APP (COVID-19 TRACKER)
ADVICE FOR SURVIVORS
#KNOWTECHABUSE

Last updated: 27 April 2020

The purpose of this advice is to help survivors of domestic and family violence or stalking to make an informed decision about whether or not to download the Covidsafe App which was rolled out in Australia from 6pm AEST on Sunday 26 April.

WESNET had computer scientists examine the Australian version of the App shortly after it was released by the Australian Government. This followed earlier advice that was based on an analysis of the Singaporean version of the App (TraceTogether).

What is it?

According to the Australian Government, the Covidsafe App is designed to help track contacts between people who may have come into contact with someone who tests positive to the COVID-19 virus.

How does it work?

The App uses Bluetooth technology to store people who are within 1.5m for 15 minutes and records the other person's name and phone number. The government has insisted that the tracing app will not track people's locations and that the data it collects will be encrypted and stored on the phones.

Should I download it?

Our advice, based on what we have seen in the Australian version, is that if you need to keep who you meet with private and your abuser has physical access to your phone or you suspect the abuser has already put some kind of surveillance app (spyware or stalkerware) on your smartphone it may not be safe for you to download the Covidsafe App.

If you wish to download the App for public health reasons, but wish to keep meetings secret from your abuser, you may wish to leave your phone at a safe distance from those you are meeting with or consider leaving it behind if it is safe to do so. The App will obviously not work in the scenario where you test positive to the coronavirus, or, vice versa, if they have the tracking App and they test positive.

What data does it collect?

Our expert advisors have examined the Australian app and found that it stores up to 21 days information on the following:

- approximately how many close contacts the user of the phone had.
- when those contacts occurred.
- how long they occurred for.
- the make and model of the phone of those close contacts.

In many circumstances, the make and model of the phone of a close contact may be enough to provide an abuser with a strong clue as to the identity of the close contact. This is particularly the case if there are multiple simultaneous close contacts - for instance if an abuser knows a survivor's mother has an iPhone 7 and her father a Samsung Galaxy S8, if those two phone models appear simultaneously in the log files, the abuser could be confident that the survivor had visited their parents.

We emphasise that to get access to this information, the perpetrator would need physical access to an unlocked phone ***in advance*** or to already have installed spyware on it, At this moment, they would also require a medium-to-high level of technical skill to interpret it.

The information stored on the Australian version of the App is not encrypted and can be read by someone who has access to the phone and a medium-to-high level of technical knowledge about how to access hidden folders that store the information. Our advisers also warned us that there are some other vulnerabilities in App which could be exploited but they would need a high level of technical expertise and access to the unlocked phone. While the information sent back to the central server if you test positive is encrypted in transit, the information is not encrypted while ‘at rest’ on the device. It is difficult to access but is not impossible.

What about at the Government storage end of things? Will my data be safe?

The Government has stated that only health authorities will be able to access the data. The app doesn't directly exchange phone numbers, it exchanges codes. The government has a master list mapping the codes to phone numbers.