World Socialist Web Site wsws.org

Australian governments pushing tracing app despite unanswered privacy-functionality questions

Oscar Grenfell
8 May 2020

Australian governments are aggressively promoting COVIDSafe, a mobile phone application that will supposedly assist contact tracers in monitoring and containing the spread of the coronavirus, despite a raft of unanswered questions about its effectiveness and the privacy of those who download it.

The app is a central component of the "back to work" campaign being conducted by federal, state and territory leaders on behalf of the corporate and financial elite. Over the past weeks, they have claimed that the country has succeeded in "flattening the curve" of infections and that this justifies the rapid elimination of social distancing and lockdown measures.

At a meeting of the national cabinet today, governments are mapping a "road out of the crisis." It will involve the easing of restrictions over the coming weeks, aimed above all at forcing workers back onto the job to ensure the resumed flow of corporate profits.

This campaign is unfolding amid ongoing community transmission of COVID-19 and indications that infections could rapidly spiral out of control. A cluster at a meatworks facility in Melbourne, for instance, has been linked to 71 cases, demonstrating the perils of compelling employees to work in factories and businesses where social distancing is impossible.

Prime Minister Scott Morrison has already acknowledged that the removal of lockdowns will result in a spike in infections. Governments have claimed, however, that they will be able to "manage the spread" of the coronavirus, with the assistance of COVIDSafe along with expanded testing. To underline the importance of the app, Morrison recently declared that his vision was for a "COVIDSafe economy."

The application is premised on ongoing community transmission of the virus. It supposedly works by logging the details of all individuals who are in close proximity to someone who has downloaded the app for more than 15 minutes. Once testing reveals an infection, contact tracers will then scour the data captured by the application and seek to identify those who have also contracted the virus.

In other words, the application will only be of use after community transmission of the virus between people who do not live together.

Commentators have noted, however, that even if it works as it has been outlined, the app will not be able to identify infections of the highly contagious virus caused by fleeting contacts in public areas. Virologists, moreover, have documented the fact that COVID-19 can be spread through inanimate objects and have stated that it remains in the air longer than first thought.

An article by technology researchers at the prestigious Brookings Institution in the US last month was bluntly headlined: "Contact-tracing apps are not a solution to the COVID-19 crisis." The researchers warned that such applications, which are being rolled-out in a number of countries, would likely be ineffective at best and "disastrous" at worst.

The researchers noted the likelihood of both false negatives, stemming from contacts with infected individuals that are not logged by the program, and false positives. As an example of the latter, they commented that automated technologies are incapable of making contextual assessments. A Bluetooth signal may be established between two phones that are separated by a porous wall, for instance, which would log a contact despite the impossibility of transmission.

The researchers wrote: "The lure of automating the painstaking process of contact tracing is apparent. But to date, no one has demonstrated that it's possible to do so reliably despite numerous concurrent attempts."

Hinting at the political calculations underlying the turn by governments to such programs, they perceptively stated: "We worry that contact tracing apps will serve as vehicles for abuse and disinformation, while providing a false sense of security to justify reopening local and national economies well before it is safe to do so."

The functioning of the COVIDSafe app is shrouded in secrecy. Australian government ministers have given wildly conflicting estimates of the take-up rate required for it to be effective.

Some have provided a figure of 20 percent, while others have cited 40 percent. It has not been clear whether the officials have been referring to a proportion of the total population, the adult population or registered smartphone users. Other government representatives have called for people to “upload” COVIDSafe, apparently ignorant that mobile phone applications are, in fact, downloaded.

Despite it being hurriedly launched almost a fortnight ago, state health officials still do not have access to the data collected. Already, federal authorities have been compelled to admit that the app does not work effectively on iPhones, which account for an estimated 45 percent of the Australian smartphone market. The Bluetooth “handshake” that will result in a contact being logged will only work reliably on iPhones if users have the app open and in the foreground, something they are unlikely to do.

While it is entirely unclear that the app will do anything to assist contact tracing, there are legitimate grounds for suspecting that it will collect vast amounts of data on the population, amid a broader assault on privacy and democratic rights.

The federal government claimed when it launched the app that it would publicly-reveal those aspects of its source code that did not jeopardise the security of the program. It has failed to do so, meaning that the population is being encouraged to download an app without any opportunity of scrutinising how it functions.

The government has also claimed that the data will be stored encrypted and will only be accessible to state health officials.

Technology researchers have questioned the claims that the app will protect users’ privacy. Jim Mussared and other developers who have sought to reverse-engineer its source code have warned that the app does not work as has been claimed.

Mussared and the groups’ findings, as summarised by *Gizmondo*, included: “Two flaws that lead to potential long-term (many day) tracking of devices; An additional flaw, which leads to limited long-term tracking as well as sharing information not stipulated in the app’s privacy policy; Another flaw provides long-term tracking as well as exposure of the user’s name, in some cases; One issue allows for permanent tracking of an iPhone even when the app is uninstalled.”

An article by two University of New South Wales academics in the *Conversation* on Wednesday documented the ways in which draft legislation that will govern the app contradicts the claims of the authorities.

Professor Graham Greenleaf and senior lecturer Katharine Kemp noted that ministers have claimed that COVIDSafe will only store the details of individuals who come within 1.5 metres of a user and are in proximity for more than 15 minutes. The legislation, however, indicates that “the app collects and—with consent of a user who tests positive—uploads to the central data store, data about all other users who came within Bluetooth signal range even for a minute within the preceding 21 days.”

The privacy concerns have been compounded by the government’s decision to provide the contract for storage and management of the data to the giant US technology corporation Amazon. This week it was revealed that the company is being paid $700,000 for its services.

As some commentators have warned, under American legislation, the US government and its agencies can subpoena data from any US-registered company, regardless of where the information originates. The federal government response to the warnings about Amazon, which has close ties to the US intelligence agencies, has been a combination of intimidation and obfuscation.

On Monday, the government filed a formal complaint to the Australian Broadcasting Corporation over a story by Dylan Welch noting that the COVIDSafe data could be accessible to US law enforcement. The government branded the article as “unnecessarily alarmist.”

Its representatives, however, have taken contradictory positions on the key issue in Welch’s story at Senate committee hearings into the app this week. Attorney-General’s Department deputy secretary Sarah Chidgey declared it was “inconceivable” that the data would be provided to a US government agency, but would not give a “100 percent guarantee” that this would not take place.

In a cynical deflection, she stated: “I can give a guarantee that it is a criminal offence under Australian law” for the data to be provided to a third party. The US intelligence agencies, however, explicitly do not operate under the domestic laws of foreign countries.

Attempting to contain growing popular concern over the privacy provisions of the app, Labor Party representatives have called upon the government to be more “transparent” and to ensure that “safeguards” are built into it. Labor, though, has played a central role in the passage of many pieces of legislation directed against encryption, targeting whistleblowers and journalists and increasing the powers of the police and the intelligence agencies.

At the state and federal level, moreover, Labor, no less than the Liberal-National Party, is spearheading the dangerous back to work campaign that the app serves to legitimise.

Representatives of the Victorian state Labor government have told the media that the Melbourne meatworks cluster may not have spread as rapidly, if COVIDSafe had been operational and all workers had it on their phones. In reality, it was the government that covered up the infections for almost three weeks in a bid to ensure that businesses remained open.

The comments, however, are a warning that workers who do not download the app will be scapegoated for the spike in infections that will result from the pro-business policies of governments.