Smartphone vs virus, is privacy always going to be the loser?

April 4 2020, by Laurent Barthelemy and Richard Lein

Smartphones can help the effort to contain the coronavirus, but do we have to let Big Brother look over our shoulder?

In Europe, officials, doctors and engineers are looking at how smartphones could be enlisted in the war against the spread of the new coronavirus.

One obvious attraction for health officials is the possibility of using smartphones to find out with whom someone diagnosed with COVID-19 has been in contact.

But can this be done without intrusive surveillance and access to our devices that store a wealth of private information?

Anonymised and aggregated

Firms can "anonymise" location data received from your smartphone by stripping out personal identifiers. It can then be presented in an "aggregate" form where individual and identifiable data points are not accessable.

Your location data is already likely being used that way by mobile operators to feed traffic information to map apps.

And it is such information that the European Commission has requested from mobile operators, which can determine the location of users by measuring the phone signal strength from more than one network tower.

In fact, mobile operators have already been providing such data to health researchers in both France and Germany.

Google, which collects large amounts of data from users of its myriad services, plans to publish information about the movement of people to allow governments to gauge the effectiveness of social distancing measures.

In particular, it will display percentage point increases and decreases in visits to such locations as parks, shops, and workplaces.

Google plans to publish information about the movement of people to allow governments to gauge the effectiveness of social distancing measures

Bluetooth sleuth

Anonymised and aggregated only get you so far. To get practical data like the people with whom an infected person has had contact, you need to get invasive. Or do you?

Singapore pioneered a method using Bluetooth. This is the technology that allows people to connect wireless headphones or earbuds to their smartphones.

If you've ever connected a pair to your phone in a public place you'll

probably have noticed the devices of others nearby.

It is this feature of Bluetooth that the Singaporean app TraceTogether exploits.

Someone who has downloaded the app and kept their Bluetooth enabled will begin to register codes from all people who have the app on their phone and come within range.

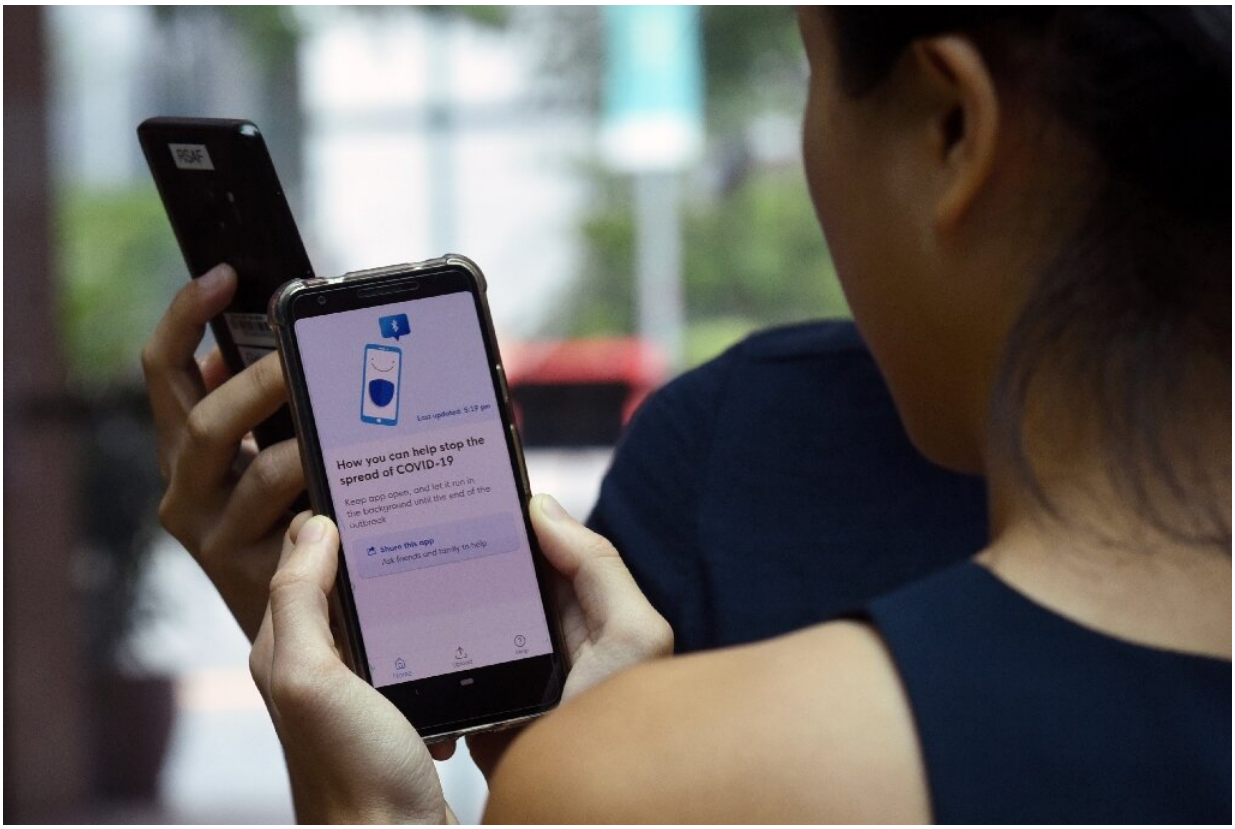
Germany is looking at rolling out a similar system.

Privacy concerns

The Singaporean app is designed to reduce privacy concerns.

For one, the app is voluntary.

Another is that it doesn't track your location, rather it just collects codes from the phones of people with whom you come into relatively close contact.



Rights groups say any additional digital surveillance powers should be necessary, proportionate and temporary

That information is only uploaded to the operator of the app when a person declares himself or herself as having come down with COVID-19.

The TraceTogether app then matches up the codes (non-identifiable except to the operator of the system) with the telephone number of owners, and then messages them they had been in contact with someone who has been diagnosed with COVID-19.

Spies in charge

The other means to get practical information is to utilise the location data of phone users.

This is the method chosen by Israel, which put internal security agency Shin Bet in charge of obtaining the data from mobile phone operators.

It also gets access to data on the movement of people for a two week period to help track down people exposed to the coronavirus.

Shit Bet does not get access to a person's phone, however.

'Proportionate and temporary'

Putting the fox in charge of guarding the henhouse is unlikely to sit well with rights and privacy groups, although they don't exclude the use of technology to help combat the crisis.

"However, States' efforts to contain the virus must not be used as a cover to usher in a new era of greatly expanded systems of invasive digital surveillance," said a statement issued Thursday by 100 rights groups including Amnesty International, Privacy International and Human Rights Watch.

They warn that "an increase in state digital surveillance powers, such as obtaining access to mobile phone location data, threatens privacy, freedom of expression and freedom of association, in ways that could violate rights and degrade trust in public authorities—undermining the effectiveness of any public health response."

They said any additional digital surveillance powers should be necessary, proportionate and temporary.

"We cannot allow the COVID-19 pandemic to serve as an excuse to gut

individual's right to privacy," the groups said.