The international journal of science / 30 April 2020

nature

COVID-19 digital apps need due diligence

Governments see coronavirus apps as key to releasing lockdowns. But they must be effective and the data secure.

In the toolkit of strategies to stop the spread of SARS-CoV-2, more countries are reaching for smartphone apps. When phones with such an app are close together, they exchange information — in some cases creating a log of who a phone's owner has been near. These 'contacts' will be alerted if they have been close to an infected person. Such apps can complement a country's overall COVID-19 control strategies — including testing, contact tracing, isolation and social distancing — but they cannot serve as a replacement for them, or the thousands of contact-tracing teams they require.

Like any health-care intervention, coronavirus apps need to conform to the highest standards of safety and efficacy. But despite the pandemic's global nature, countries are developing apps independently, and there are no global standards — which is rightly raising concerns.

Some countries are already starting to use phones to record data, including names, addresses, gender, age, location, disease symptoms and COVID-19 test results. For example, users of Australia's COVIDSafe app, launched last weekend, will be contacted by health officials if an app user they have had close contact with tests positive for COVID-19. Germany's app, which is still in development, will also use actual test results. Australia is storing data centrally, but, after much debate, and expressions of concern from researchers, Germany's app will store coronavirus data on individuals' phones. Egypt's app, launched earlier this month, uses a phone's location services to alert users if they have been near anyone with COVID-19.

Use of all of these apps is voluntary, as it should be. In most cases, the apps are being developed by governments working with technology companies and researchers. But, considering that citizens are being asked to give up their personal data, there has been little national public consultation. Another cause for concern is the fact that there is scant published evidence on how effective these apps will be at either identifying infected people who have not been tested or, if widely used, stopping the spread of the disease. Governments are excitedly pointing out the benefits, but are saying less about the risks.

Key questions need answers

One serious concern is accuracy. Apps that link to official validated tests are more likely to give accurate results. An alert based on self-diagnosis that turns out to be wrong — a false positive — could, of course, be corrected. But if incorrect information has been sent to a large group of contacts, it will have caused unnecessary alarm, and could have wrongly sent people into isolation for weeks.

> **"Apps should not be rolled out without pilot studies or risk assessments being published."**

An equally important concern is privacy. As we have pointed out before, it is becoming easier to identify individuals from anonymized data sets. Researchers have shown that it is possible to re-identify individuals even when anonymized and aggregated data sets are incomplete (L. Rocher *et al. Nature Commun.* **10**, 3069; 2019).

Researchers are also raising concerns about the decision some countries have taken to store data centrally. Earlier this month, nearly 300 researchers signed an open letter reminding governments that data stored on individual phones are more secure, and that data stored centrally are more susceptible to hacking.

COVID-19 apps have, to some extent, been inspired by the experiences of South Korea and Singapore. South Korea, in particular, is regarded as a model because it avoided severe lockdowns. Some 3 months after the outbreak spread to the country, only a handful of new cases are being reported daily and 244 deaths have been recorded in total.

But the foundation for South Korea's COVID-19 response is a comprehensive testing strategy, backed by a nationwide network of contact-tracers who interview infected people and trace their contacts. The strategy includes the use of phone alerts, but not the type of phone app being developed elsewhere. More importantly, it is based on a degree of surveillance that people in many other countries would find hard to accept.

When a person tests positive for COVID-19, a text alert is sent to everyone living nearby. The alert typically includes a link to a detailed log of the infected person's movements — in some cases to the nearest minute — which are reconstructed from public data, such as closed-circuit television cameras. But the government is also permitted to access confidential records, such as credit-card transactions. The data are then stored centrally by government agencies.

Much attention has also been paid to Singapore's app, which now has more than one million users — roughly one-fifth of the population. But it still means that in any encounter between two randomly chosen people, there is only a 4% chance that both will have the app. This points to one of the deepest flaws in digital contact-tracing plans anywhere: the fact that only a fraction of any population is likely to have the app at all. And such efforts will miss out anyone who, for any reason, doesn't have a smartphone.

It's not that digital contact tracing shouldn't be done, but it should not be a substitute for human contact-tracing teams; nor should it be seen as a replacement for necessary COVID-19 testing. And apps should not be rolled out without pilot studies or risk assessments being published.

Speed is, of course, of the essence — but so is due diligence and due process. This includes public dialogue; more involvement from researchers, including those who study ethics, law and public engagement; and a cast-iron commitment from governments that the information being harvested is secure and will only ever be used for the reasons it is being requested.