TOMORROW'S
CHALLENGES

CORONAVIRUS: DIGITAL CONTACT TRACING DOESN'T HAVE TO SACRIFICE PRIVACY

By José Parra-Moyano, Professor Karl Schmedders and Michel Avital

Chemin de
Bellerive 23
PO Box 915,
CH-1001 Lausanne
Switzerland

Tel: +41 21 618 01 11
Fax: +41 21 618 07 07
info@imd.org
www.imd.org

Pressure is building on governments around the world to reduce the lockdown measures used to stop the spread of COVID-19, and to prevent the disease re-emerging once it is under control. As a result, there are many proposals to use data from people's smartphones to track their movements and contacts with potentially infected patients, in order to trace anyone who is likely to have caught the virus. Other systems involve monitoring the data trails of all citizens to generate useful information that helps to prevent the spread of the disease.

All these approaches involve allowing the government, and in some cases private companies, to build a database of where we go, the people we associate with and when. Such intrusive tracking is more typically associated with totalitarian regimes and easily can be misused. Despite the good intentions, then, these measures raise serious concerns that collecting and sharing such data might pose a threat to citizens' right to privacy.

The severe threat of COVID-19 makes it vital that we share information in order to fight its spread. But as a society we have a choice about how and under what terms we share our data. We can do it blindly without knowing who will use our data and for what purpose, diving deeper into the age of surveillance capitalism and risking our personal freedom.

Alternatively, we can develop a data consciousness, becoming aware of the power of our data, taking control over it, and reshaping the way it is handled. But this may still involve giving up our privacy. But there is technology that could help to resolve the inherent tension between the need to share data and the need to protect it from misuse.

Zero-knowledge proofs

One of these technologies is based on a set of cryptographic protocols known as zero-knowledge proofs (ZKPs). ZKPs are a way of encrypting data that allows the owner of data to display an attribute about it and prove that it is accurate without revealing the data itself. For example, by means of a ZKP, a citizen can prove that he or she is adult, without revealing his or her age.

In the context of preventing a pandemic or gradually relaxing the lockdown, ZKPs can be very useful. They could allow people to prove that they have had no contact with a known infected person without disclosing exactly who they have interacted with. Similarly, they could prove that someone hasn't been in an area of high infection risk, without showing where they have been. This is sharing information without sharing data.

ZKPs could be incorporated into some of the systems that are already tracking people's mobile phone geolocation to determine where they have been and who they have encountered. South Korea, Israel and other countries have already implemented mobile phone tracking that could do so.

Other countries, such as Singapore, are using dedicated smartphone apps that don't track your location but do record how close you get to others using Bluetooth. Incorporating ZKPs into such systems would decrease the privacy risks associated with them by allowing people to share whether they have encountered an infected person without sharing where and who this person was.

Another technological approach to protecting privacy builds on the idea of decentralised architecture. This essentially means tracking apps would not need to store locations or contact data in a central repository. Instead, all tracking data would be stored locally on your phone and linked to a unique private key. If you were diagnosed with COVID-19, you could ask the app to send an encrypted message to all the phones with which you had come into close contact.

This would allow a peer-to-peer sharing of infection risk while protecting everyone's privacy and avoid the need for any central authority to oversee the data. ZKPs could also be incorporated into such tracking and messaging systems.

Apple and Google are reportedly collaborating on a contact tracing app that uses such a decentralised approach. But some countries, including France and the UK, have so far rejected the idea in favour of systems that allow authorities to gather more data.

We face a situation where governments are responding to the possibilities of using technology to fight a pandemic by gathering even more data about their citizens than they already do, risking a crucial infringement of their rights. We urge citizens and governments to think about the unintended consequences of massive data sharing and to be aware of the tension that has with personal privacy.

This article is republished from The Conversation under a Creative Commons license. Read the original article here.