Digital surveillance can help bring the coronavirus pandemic under control—and threatens privacy

10 April 2020, by Jennifer Daskal

Some people might choose to use their mobile phones to prove they're abiding by quarantine orders rather than have police officers check up on them. Credit: 28704869/Flickr, CC BY

Israel's top spy agency has been using secretly collected cellphone data to retrace the movements of those who tested positive for the coronavirus.

The Polish government launched the "Home Quarantine" app so that people in quarantine can upload geo-located photos proving they're at home.

The South Korean government is using a combination of mobile phone data, credit card information and facial recognition software to track the movements of people who test positive for COVID-19. The government posts the details publicly to alert people who might have come in contact with the infected person.

Public health benefits? Certainly. Privacy risks? Certainly as well.

As a technology, law and security scholar at American University Washington College of Law, I study questions of privacy and surveillance. The pandemic is confronting Americans with important questions about how much and what kinds of surveillance and tracking to accept in support of better health, as well as a revitalized economy.

Deaths in the U.S. from the coronavirus are projected to reach six digits, which adds urgency to decisions that have long-term consequences. Should location data be used to identify and warn those who have been exposed to the virus? Data be used to enforce quarantines? Can digital information be used to serve compelling health needs without boosting the reach of the surveillance state?

Already, cellphones, apps and digitally connected devices provide a range of data that can be used to track movements and associations with varying degrees of specificity. Though some of this digital surveillance requires users to opt-in to data collection, a lot is already in the hands of companies that are now using it to predict trends.

A smart thermometer company, for example, is using real-time temperature data to forecast the next COVID-19 hot spots, something it's done successfully to predict the seasonal flu. Google has been compiling data from Google Maps to chart shifts in people's movement over time. The company is repurposing data used to predict traffic flows to help officials determine how well the population is engaging in social distancing. Both are examples of population-level analysis, using aggregated data to assess trends in ways that, if designed and implemented properly, can provide important health information while also protecting

personal privacy.

Tracking individuals

Things get more complicated, however, with the move from aggregated analysis to individual-level tracking. There are, broadly speaking, three key forms of individual tracking being pushed, each raising unique policy and legal considerations.

The first, contact tracing, is used to map the movements of sick individuals in order to warn unsuspecting contacts so they can take appropriate steps to protect themselves and others. The second uses location- and time-stamped photos to monitor compliance with quarantine orders and travel restrictions. The third identifies and tracks those who have tested positive for SARS-CoV-2 antibodies. This type of tracking—being contemplated in Germany and England – could be used to provide immunity passes to allow people who are no longer at risk to return to work or otherwise engage socially.

Several universities, companies, nonprofit organizations and governments are developing contact tracing apps that identify when someone has been in contact with other people who have tested positive for the disease. Stanford University-based COVID Watch, for example, is developing an app that uses Bluetooth technology to map where and when people cross paths, which can then be used to anonymously notify those who have had contact with sick people who have a compatible app. This is an open source, decentralized system, without the need for any government data collection. Singapore's TraceTogether app is also an open source system that relies on Bluetooth technology to map associations and issue warnings.

These kinds of decentralized tracking systems are designed to better protect privacy than government-collected or other centrally maintained datasets. But these apps are opt-in, meaning people have to actively choose to use them. As a result, they will only be as effective as they are widespread, something that depends in part on whether users trust the security and other privacy protections built into the system design.

Data collected by smart thermometer companies can give public health authorities warnings of potential disease outbreaks. Credit: Julien G./Flickr, CC BY

Check-ins and blood tests

Other forms of tracking raise both privacy-related and other civil liberties considerations. Quarantine monitoring systems like Poland's Home Quarantine app or Singapore's quarantine requirements, coupled with twice daily digital check-ins, raise the specter of Big Brother, achieved via digital monitoring.

In the United States, this kind of monitoring runs up against the Fourth Amendment's protections against unreasonable search and seizure. But the Fourth Amendment is not an absolute. Digital monitoring could be court-ordered in response to someone's demonstrated failure to abide by criminally enforceable quarantine orders, many of which are now in place.

Meanwhile, the police could be employed to knock on doors and check compliance with quarantine orders—even in the absence of a demonstrated failure to abide by the orders. Individuals could, as a result, presumably consent to digital monitoring as an alternative to daily check-ins by police. Depending on the design, digital check-ins might also be deemed valid under the "special needs" exception to the Fourth Amendment. In such cases, the central question is the validity of the quarantine

orders rather than the means of enforcement.

Meanwhile, even the seemingly innocuous tracking of those who test positive for antibodies may not be as innocuous as it seems. If and when such testing becomes reliable and available, it could provide critical, albeit imperfect, assurances on both the individual and community level. But whereas aggregate-level analysis can help determine when it's appropriate to lift restrictions, individual tracking risks dividing communities into groups of "clean" and "dirty," with privileges doled out according to status.

Principles for protecting privacy

As society works through these difficult issues, a few key principles should guide decision-making.

First, design matters. Tracking systems should, to the extent possible, be open source, decentralized and designed in a way to share the key health data without gathering or revealing the movements and contacts of those involved. The best contract tracing apps do just that, incorporating key principles of privacy by design and back-end limitations on things like who can access the data and to whom it can be disseminated. Importantly, data should not be retained any longer than it is needed.

Second, whatever system is put in place, whether privately developed or government-mandated, it should be carefully tailored to serve a specified and compelling health need.

Third, any claims that governments need new authority should be examined carefully and warily, particularly given the trove of data already available. If adopted, any new authority should be explicitly time limited, with clear and constrained criteria for extending the time limits.

When the last massive pandemic hit a century ago, the population did not walk around with tracking devices. Now we all do. This is data that can both protect people and confine them. It should be used to save lives but in ways that also protect core freedoms.

Provided by The Conversation