The app credibility gap

A slew of national COVID-19 exposure apps have failed because of poor public engagement and acceptance. Apps from the workplace may offer a partial solution if privacy can be guaranteed.

On 16 June, only two months after its launch, the Norwegian Public Health Institute (FHI) withdrew its coronavirus tracking app Smittestopp (Infection Stop) after warnings of over-intrusiveness from the government's cybersecurity department, the Norwegian Data Inspectorate. FHI's director, Camilla Stoltenberg, announced that all data collection would stop and any data gathered to that point would be destroyed. Smittestopp is one of many national COVID-19 tracking apps to flop due to a lack of public engagement and acceptance. As economies reopen, a growing number of employers and local institutions are offering apps to their constituents. These apps may offer a solution to the widespread lack of public uptake of digital tracking technology until now.

At least 35 nations around the globe have launched COVID-19 apps intended to transform contact tracing of SARS-CoV-2 outbreaks. Across the board, however, adoption has been low. According to MIT Technology Review, in Iceland, a country that prides itself on an informed citizenry and open information systems, only 38% of people downloaded the app. In Singapore, the number was only 25%, in Australia 21% and in Israel 17%. Elsewhere, uptake has been below 10%, and often below 1%. Tracking apps need to be deployed by 60–80% of a population to be effective epidemic-control tools.

Given the widespread failure of digital health apps to gain traction, the concern now — with political and economic imperatives to reopen, a growing fatigue of social distancing and waning public fear of the disease — is that other nations will follow Norway's lead and dump their apps — and their app data. If so, an opportunity to capitalize on app-generated real-world data to understand the mechanics of SARS-CoV-2 transmission and the impact of non-pharmaceutical interventions (such as social distancing, travel restriction and reopening) will be lost.

Development of Smittestopp was stopped because, according to Amnesty International, the decision to collect and store app data on centralized government computers ran "roughshod over people's privacy, with highly invasive surveillance tools." Voting with their index fingers, most Norwegians seemed to agree. Although a quarter of the population downloaded Smittestopp in just a few days after launch, only a third of those 1,343 million users bothered to activate it. With under 10% of the population using the app in a country with an already-low COVID-19 incidence, Smittestopp was doomed.

The uptake of other COVID-19 apps around the world has similarly been disappointing. This is due to a shift in public priorities, skepticism about the effectiveness of mobile tracing technology and a lack of trust in government.

In April and May, at the height of the epidemic in Europe and the United States, a series of surveys of around 6,000 people indicated that 70–80% would "definitely install" or "probably install" tracking apps. But as infections fell, fears about SARS-CoV-2 subsided and skepticism about the effectiveness of apps rose — as demonstrated by responses to the Robert Koch Institute's COSMO survey — uptake and use has fallen.

One of the public's biggest concerns is privacy. A Johns Hopkins University/Microsoft Research survey of some 5,000 US respondents indicated that 82% would use a "perfectly accurate and private" tracing app, but only 24–26% would want one with even "a low chance" of a data leak to the government, an employer, a tech company or a non-profit organization. Recognizing these concerns, developers have committed to open-source rather than proprietary code, dumped the use of location data and adopted measurements of phone-to-phone proximity through encrypted low-energy Bluetooth signals.

A new protocol called decentralized privacy-preserving proximity tracing (DP3T) now sits behind apps being developed in Estonia, Finland and Switzerland, whereas other European countries are working with the Apple and Google API. Both APIs process data on users' phones rather than sending the data to central computers, government or otherwise; both make users primarily responsible for alerting health authorities to changes in symptoms and disease status.

Unfortunately, if low uptake of apps continues, none of the above will matter. The failure of infection-tracking apps will become a self-fulfilling prophecy: apps cannot work if too few people install them, and people won't install them if they think apps don't work. An exit from this futile cycle will need a reappraisal of human social behavior.

Following reopening, citizens are likely to restore at least some elements of their routine lives. Encounters between people will increase, the vast majority occurring at nodes (such as schools, places of worship and workplaces) and connections between those nodes and home (for example, mass transit routes, shops, malls, gyms, cinemas, bars, nightclubs and restaurants).

With little appetite for broad public uptake of apps, the onus falls on those controlling the nodes — employers, deans, school principals, pastors — to encourage their workers, pupils or congregants to use their apps. In turn this will help track infections and ensure individual isolation at the local level, better ensuring the safety of the many.

In the United States, there are some first signs that this approach is being adopted. In partnership with MyOwnMed, Drexel University is offering a Health Tracker app to report whether essential employees are experiencing COVID-19 symptoms. Similar efforts between Gozio Health and the University of Texas, San Antonio and between Microsoft and Baylor College of Medicine are underway. In the private sector, UnitedHealth Group and Microsoft are offering to US employers a free COVID-tracking app compliant with the US Centers for Disease Control guidelines.

Of course, the absence of a coordinated tracing capacity at the municipal, regional and national level will mean that certain groups — particularly low-income, unemployed individuals without access to smartphone technology — may fall beyond the reach of these COVID-19 tracking apps. And many do not want to share personal health information with their employer. But in the face of widespread evidence of the failure of tracing apps to engage with people in democracies, targeting digital technology to organized groups may be a compromise worth making. ❐

Published online: 26 June 2020
https://doi.org/10.1038/s41587-020-0610-4