JOHNS HOPKINS BLOOMBERG SCHOOL of PUBLIC HEALTH | Center for Health Security

Review of Mobile Application Technology to Enhance Contact Tracing Capacity for COVID-19

April 8, 2020

Contact tracing is a mainstay of a robust public health response. The purpose of contact tracing is to identify potentially exposed (and therefore potentially infected) individuals so that they can be quarantined before they develop symptoms, thus preventing further transmission in the community. The pace of the COVID-19 outbreak in the United States has quickly overcome existing public health infrastructure and highlighted the need for an innovative solution to increase contact tracing capacity. Several countries have used technology to scale up these capabilities. A modeling study conducted by a team in Oxford, UK, demonstrates that, with the use of technological solutions, it is possible to drive the rate at which infections are reproduced below a threshold needed to halt the spread of COVID-19.

Here we review prominent apps developed to support contact tracing for COVID-19. We do not provide recommendations or examine the privacy or security implications of these technologies. Most technologies developed to support contact tracing have been designed to alert individuals when they have been in the vicinity of a known COVID-19 case.

The first technology was implemented in China and functioned as a "close contact detector." Through the use of QR codes scanned by users and government identification numbers, the app integrates with the Ministry of Transport, China Railway, the Civil Aviation Administration, and the Chinese National Health Commission database. Once the user has entered his or her identification number, the app will alert the user with instructions to stay home and contact health authorities if the user has been in the same space as someone who has a confirmed infection. The success of this surveillance strategy has been based on previously existing infrastructure monitoring the movement of people within China. The app can provide potential exposure information for the previous 2 weeks. The app is also intended to be used to determine the ability of individuals to move throughout the country, based on their exposure history.

Similarly, in the Republic of Korea, technological approaches to contact tracing primarily rely on the location data of an individual's mobile device. The Corona Map and Corona 100m apps use data from government information systems, including those from the Korea Centers for Disease Control, to send push notifications if the user has been within a certain distance of a person known to be infected. The notifications provide detailed information on the individual the user was exposed to, including age, sex, and location of the exposure. This method relies on location data and government-managed databases and individual identification numbers. The app will also map locations with higher concentrations of known cases to direct individuals to avoid these locations. The app integrates GPS history, data from nationwide surveillance cameras, and credit card transactions.

The applications in both China and the Republic of Korea rely on personal identification information combined with location histories. Alternatively, the TraceTogether app developed in Singapore uses short-distance Bluetooth signaling between devices to detect users in close proximity. The data are then stored on the individual user's device and can be sent to the ministry of health to supplement contact tracing efforts. This app does not collect any location data, either from the individual or where the contact happened, and the data are not automatically sent to the government. The data will be released only with the consent of the user in the event that the user is infected. After a period of 21 days, all data collected are automatically deleted.

In Europe, efforts are under way to develop a GDPR-compliant platform to enable contact tracing using an approach that enables full anonymity; it is called Pan European Privacy-Preserving Proximity Tracing (PEPP-PT), and each user is issued an anonymous ID. Like other privacy-focused approaches, PEPP-PT relies on Bluetooth, rather than geolocations, to measure proximity. This technology does not appear to be operational yet.

In the United States, there have been 3 primary initiatives to develop mobile applications to assist with contact tracing. The apps prioritize privacy and focus on enhancing contact tracing without potentially exposing individual identity or generating stigma around certain businesses or establishments.

COVID-19 Watch from Stanford University uses Bluetooth signaling to detect other users in the area and will alert users anonymously if they were in contact with someone who was confirmed to be infected with COVID-19. The data are collected voluntarily and are anonymized. The goal is a 3-pronged approach: (1) contact tracing with automated alert of contacts based on short-range Bluetooth signaling; (2) heatmaps based on anonymized GPS data on locations of higher concentrations of cases to identify high-risk areas for transmission; and (3) generation of risk reduction strategies for health practitioners based on the data.

The second group is CoEpi: Community Epidemiology in Action, which is also a voluntary, Bluetooth-based contact tracing application that includes self-reported symptom sharing to support exposure notification even before confirmation of test results.

Finally, the Massachusetts Institute of Technology developed Private Kit: Safe Paths, which can be used by both individuals and health authorities to enhance contact tracing. The app can be integrated with Safe Places, which collects time-stamped location data using Private Kit: Safe Paths data, Google locator history, and individual interviews conducted by health departments. All data are stored locally on the user's device and encrypted for individual users. In the event of a confirmed case, a GPS trail can be released with the consent of the user. The app will enable notification of users who have crossed paths with a confirmed case. The application does use GPS location data, which is encrypted to protect individual identity and is released only if the user who is a confirmed case chooses to share the data with health officials.

