Debevoise & Plimpton

Debevoise In Depth

CORONAVIRUS RESOURCE CENTER

Can Contact Tracing Apps Help Get Many of Us Back to Work Soon? A Framework for Evaluating the Various Options and Legal Concerns

April 24, 2020

Each passing week of lockdown brings mounting economic and social costs, increasing the urgency to find ways to get more people back to work safely. A large part of that effort involves the development of contact tracing applications ("apps") for mobile phones. These apps promise to allow low-risk individuals to return to some normal activities in the near term while continuing to isolate those with higher risks.

China, Hong Kong, Israel, Singapore, South Korea and Taiwan have all had varying degrees of success in using electronic contact tracing (along with widespread virus testing and manual contact tracing conducted by health professionals) to allow a significant portion of their population to return to school and work, albeit with limitations.

In regions that have not yet implemented contact tracing apps, there are several models being considered, the most publicized of which is being developed through a partnership between Apple and Google. Each model generally involves the collection of health and/or location data. Most models then use that data to quickly identify individuals who recently had close interactions with someone who tested positive for the virus. The specifics of the various models, however, differ dramatically. There are models that involve mandatory, government-controlled collection of vast amounts of sensitive medical and location data in order to identify, quarantine and track the movements of people who are likely infected. By contrast, there are also models that are voluntary and decentralized, designed only to alert individuals of their increased risk of infection. Such apps merely recommend a course of action. In between those two extremes are several options that make different choices with respect to eight variables discussed below.

For each variable, developers must try to balance several competing interests:

- The rate of adoption;
- The risk of deliberate or inadvertent recording of false data;
- Limiting the number of people who are misclassified as either low-risk or high-risk;
- Protecting the legitimate cybersecurity, privacy and constitutional concerns of individuals; and
- The overall ability of the program to allow more people to safely increase their mobility.

Striking the right balance among these competing objectives will require difficult choices as to what data will be collected, how it will be collected, who should have access to it and how the collected data should be used. In an effort to provide a framework for evaluating these choices, we have assembled the following considerations for assessing electronic contact tracing apps.

Voluntary or Mandatory

- Some countries, such as Israel, are leveraging their government's anti-terrorism capabilities to create a mandatory centralized tracing program.
- For a variety of legal and cultural reasons, however, it is unlikely that a fully mandatory system would be viable in the United States, the EU or post-Brexit UK. Currently, most European and North American proposals have individuals voluntarily download the tracing app to their mobile phones.
- But the voluntary or mandatory choice is not binary. Some programs are voluntary for the general population, but become mandatory for those testing positive or arriving from abroad and are therefore ordered into quarantine (*e.g.*, South Korea and Taiwan).
- Even fully opt-in programs can take on a quasi-mandatory character if participation creates significant advantages. (*e.g.*, if entry into certain large venues – such as concerts or sporting events – depends on it, or if restaurants and movie theatres offer large discounts or priority access to people who are determined to be low-risk by the app).

- In general, the more mandatory the program and the more government involvement, the more likely it is to face scrutiny in the United States under the Fourth and Fourteenth Amendments, and in Europe under the European Convention on Human Rights and the European Charter of Fundamental Rights, as well as Member States' constitutions and domestic law.

GPS or Bluetooth (Centralized or Decentralized)

- All contact tracing programs utilize some form of location data. Some track specific locations on a map using GPS data (*e.g.*, South Korea and Taiwan), while others rely on Bluetooth to provide only relative location data (*i.e.*, Phone A and Phone B have come in close contact with Phone X and Phone Y).

- The collection of GPS location data raises privacy and cybersecurity concerns in the United States and Europe because it can reveal sensitive personal information about individuals, such as visits to a psychiatrist. GPS technology is also somewhat limited in determining precise locations indoors and in areas with many large buildings.

- By contrast, Bluetooth models, such as the Apple/Google proposal and the contact tracing app used in Singapore, do not track specific locations and are therefore considered to have less cybersecurity and privacy risk.

- In Bluetooth-based programs, when phones that have downloaded the app come within a certain short distance of each other for a specified period of time, they exchange certain identifiers. If an individual later records a positive test for COVID-19 in the app, all the phones that recently received an identifier from the infected individual's phone are notified.

- The shorter the distance and the longer the time period selected for triggering an alert, the fewer number of false positives (*i.e.*, the fewer people receiving alerts who are unlikely to be infected). The longer the distance and the shorter the time period selected for triggering an alert, the fewer number of false negatives (*i.e.*, the fewer number of people who are likely infected who do not receive an alert).

- In general, GPS-based tracing is centralized, while Bluetooth tracing can be decentralized, with the data residing only on the phones of the participants. But Bluetooth tracing data can also be collected from participants and centralized by a government agency, which is the approach being pursued in Germany and France.

Positive Test Results: Self-Reporting or Verified Recording

- In many proposals, patients who test positive are encouraged, but not required, to record their results in the app. The obvious concern with self-reporting is that some people will not do so.

- A less obvious concern is that some individuals may falsely record a positive result when, in fact, they tested negative or have not been tested at all. People may do so to negatively impact people with whom they have recently been in contact (such as a business competitor or estranged former romantic partner), or so that they can later claim immunity.

- To address these concerns, some models only allow medical professionals, or individuals with secure codes received from testing facilities, to record test results in the app. (*e.g.*, Singapore).

Consequences of Confirmed Contact with an Infected Person

- For most models, when a person participating in the program tests positive for COVID-19, other program participants with whom that person has been in close contact in the previous 14 days are now considered "high-risk" and are contacted.

- In some models, those high-risk persons are contacted automatically through the app, informed of their possible exposure and told that they should be tested, contact health officials and/or enter self-quarantine. (*e.g.*, South Korea). In other models, high-risk persons are contacted by a healthcare professional who informs them that they have been ordered into quarantine. (*e.g.*, Singapore).

- Some apps only provide the most basic information as to why high-risk individuals are being contacted. (*e.g.*, Israel's Hamagen app sends a message alerting the individual of "points of intersection found with coronavirus patient").

- Other apps, such as those used in Singapore, provide more details, including the day and location of the contact. One of the apps used in South Korea also provides the age and sex of the person who tested positive.

- Depending on the number of recent contacts that the notified person had, such detailed alerts may lead to the identification of someone who has tested positive, which creates privacy concerns over the disclosure of sensitive medical information and also risks panic, stigmatization and possible violence against that person.

Other Uses

In addition to notifying potentially infected individuals, some contact tracing apps are used for a variety of other COVID-19-related functions, including:

- Enforcement of quarantine by requiring isolated persons to have their phones with them and turned on at all times, and to respond to periodic check-in calls. (*e.g.*, Taiwan).
- Monitoring adherence to social distancing requirements. (*e.g.*, Israeli company Viziblezone is developing an app that would use phone signals to alert a user when they are too close to another individual).
- Imposition of travel or work restrictions for people who are determined to be high-risk by the app or cannot show compliance with government orders. (*e.g.*, people who do not download the app, do not have their phones with them or travel with their phone turned off or in airplane mode).
- Collection of symptom information, which could come from only those who have tested positive, those who are in quarantine or all users of the app. This could be enhanced by providing individuals with smart thermometers connected to the app. This information could be used to assist in the allocation of medical resources for specific locations. If, for example, many people in a certain location are observed not to be social distancing and are recording fevers or other symptoms of COVID-19, hospitals in that area may start preparing for additional cases.
- For those people who have tested positive and recovered, the app also could be used to identify those who likely have some form of immunity and who, therefore, may no longer need to adhere to social distancing requirements.

Providing Real-Time Data

- One difficult choice is whether the app should provide real-time data. If, for example, Person A's phone comes in contact with the phone of Person B, who has recently tested positive (and is in a public location contrary to quarantine instructions), should Person A be alerted in real-time? Such an alert may be extremely valuable to Person A who, due to age or medical condition, may be particularly vulnerable to COVID-19 and would therefore want to leave the location to avoid infection.

- But such an alert could also reveal the identity of someone who has tested positive. That kind of disclosure of medical information creates privacy and possibly safety concerns for the infected person. As such, real-time notifications may dissuade some individuals with symptoms from getting tested or visiting the hospital, which is contrary to the goals of the contact tracing program.

Security and Transparency

Security and transparency are issues for several aspects of these programs, including:

- What will the data be used for, and who, if anyone, has access to individuals' location and testing data, including agencies in the government, law enforcement, healthcare workers, employers and others?
- What are the exact parameters (distance, duration, etc.) that will trigger an alert based on interactions with a person who later tests positive?
- Will the code of the app itself be made public?
- What data security measures, including encryption, have been put in place to ensure that the data will not be hacked or leaked?
- Will the data collected be deleted at some point? If so, when? Who will ensure that it is deleted, and deleted securely?

Governance and Oversight

- Some have expressed concerns that the ability to force individuals or groups of people into isolation could be abused and have demanded a measure of legislative or judicial oversight for the programs. (*e.g.*, in Israel, citizens and privacy advocates challenged the use of GPS data by the government's Security Agency to track confirmed cases and enforce quarantine protocols. The Supreme Court upheld this program with the stipulation that a parliamentary committee be tasked with overseeing it). Press freedom groups have cited the risk that governments hostile to the media could use these technologies to track journalists.
- For programs that enforce quarantines, some have also called for an appeals process to contest individual lockdown orders, especially when no information is provided as to why quarantine has been imposed on a particular individual.

General Criticisms

There are some criticisms that apply to all electronic contact tracing models, regardless of the choices made with respect to the variables discussed above. These include:

- The programs do not work for those who do not have their own smartphones, which is true for many elderly and lower-income individuals.
- All of these technologies are imprecise and will result in false positives – *i.e.*, people who are mistakenly identified as high-risk who, in fact, have had no exposure to an infected person. One example is someone who has not left their apartment building in weeks. That person may have been in close proximity to an infected neighbor for an extended period of time, but on the other side of a thick concrete wall that the tracing technology cannot discern.
- There will also be false negatives – interactions that result in the spread of the virus that go undetected, perhaps giving some people misplaced confidence to relax social distancing because they have not been sent alerts by the app.
- There will also be significant software and hardware difficulties, including: a lack of compatibility between phones using different operating systems, difficulties processing updates, and functionality issues due to locked phones, limited battery life or poor Internet connections.

All of these issues will need to be addressed in some way in order for the apps to be both widely adopted and effective.

Conclusion

Electronic contact tracing apps are likely to be one part of successful back-to-work programs, which will also include widespread testing, manual contact tracing, continued social distancing and early symptom detection. There are cybersecurity, privacy and constitutional concerns about these apps because they have the potential to collect and disclose sensitive medical and location data. Those concerns have to be weighed against the effectiveness of some of these apps in hastening our ability to return to work or school in large numbers. If some cities are able to relax their social distancing requirements in part because of their contact tracing programs, pressure will mount on other cities to adopt similar measures. It will take care and creativity to implement electronic contact tracing programs that are widely adopted, effective at identifying high-risk individuals and adequately address legitimate cybersecurity, privacy and constitutional concerns.

* * *

For more information regarding the coronavirus, please visit our Coronavirus Resource Center.

Please do not hesitate to contact us with any questions.

Luke Dembosky
ldembosky@debevoise.com

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Anna R. Gressel
argressel@debevoise.com

Joshua B. Pickar
jbpickar@debevoise.com

Suchita Mandavilli Brundage
smbrunda@debevoise.com

Samantha B. Singh
sbsingh@debevoise.com