Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

May 29, 2020

Digital Contact Tracing Technology: Overview and Considerations for Implementation

Background

"Contact tracing" is a public health measure used to control disease spread. Trained public health workers assist patients with an infectious disease recall their close contacts within a given timeframe, notify them of potential exposure, and provide advice to patients and contacts. Given the scale of the COVID-19 pandemic, some public health authorities are automating part of the tracing process with smartphone applications (apps). Some apps take advantage of Bluetooth signals to track individuals proximity to one another, otherwise known as "digital exposure notification (DEN)" Bluetooth allows short-range wireless communications between electronic devices. Apps may also be used by public health authorities to enable "digital contact tracing" (DCT), which may also use location data.

Development of DCT and DEN Apps in the United States

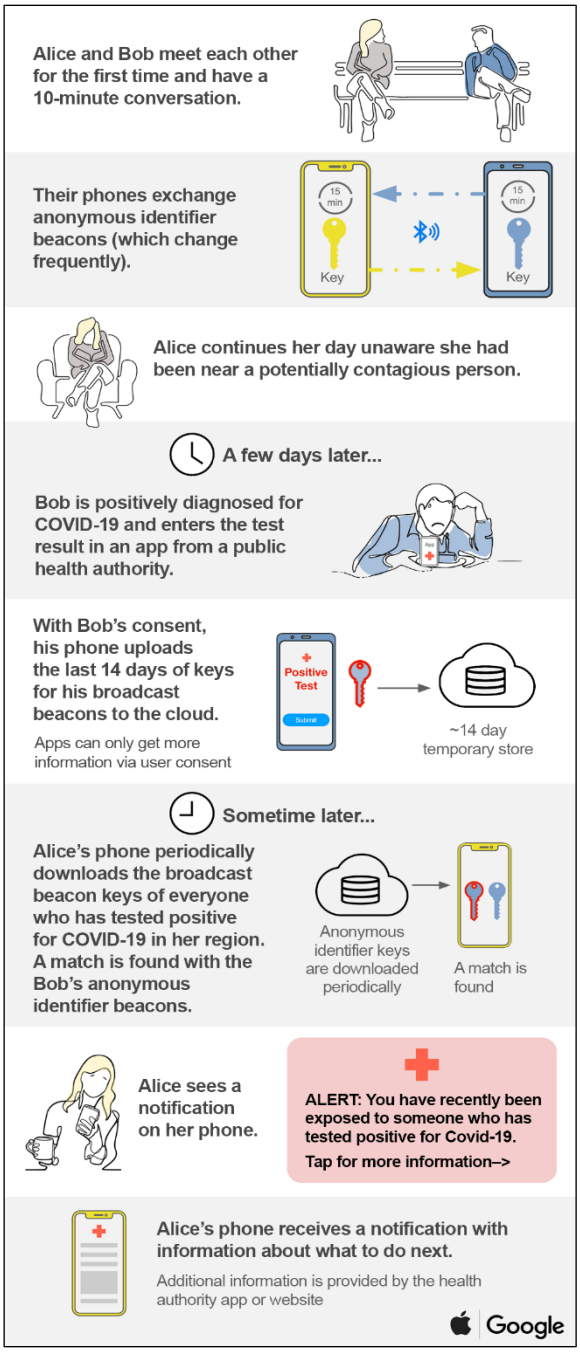
In response to the COVID-19 pandemic, several countries have developed nationwide apps to support contact tracing among their citizens. Singapore developed and adopted both the BlueTrace protocol and TraceTogether app. Although the app is used only in Singapore, its Government Technology Agency has made the BlueTrace protocol available to other countries; Australia has adopted the protocol for its app. South Korea, Bulgaria, Iceland, Germany, and France are among the countries that have released or are developing nationwide apps.

The United States has taken a decentralized approach, with states engaging the private sector to develop tracing tools. North Dakota, South Dakota, and Utah have independently deployed DCT apps using both location data and Bluetooth signals. Companies such as PricewaterhouseCoopers and Salesforce are developing apps to allow corporate clients to track the proximity of their employees within an office or on a campus. In both contexts, if a citizen or employee tests positive for COVID-19, other individuals who may be at risk can be identified and contacted. The possibility of widespread, and perhaps mandatory, monitoring, whether by the public or private sector, has drawn scrutiny from privacy advocates.

Apple-Google Collaboration

On April 10, 2020, Apple and Google, which develop the iOS and Android mobile phone operating systems, respectively, announced a partnership to develop a protocol to support the development of digital exposure notification apps that use a smartphone's Bluetooth signal. The protocol will work on both operating systems, which account for nearly the entire share of the U.S. mobile phone market. It was released to developers on May 20, 2020. **Figure 1** illustrates how apps built using the Apple-Google protocol are planned to work.

Figure 1. Apple-Google Digital Exposure Notification Using Bluetooth



Source: https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf.

In the United States, users must download and opt in to an appropriate state or regional tracing app as well as opt in to

the Apple-Google tracking feature in the operating system. Once enabled, a person's smartphone will exchange anonymous identifier beacon keys with nearby smartphones using the Bluetooth signal. According to both companies, personally identifiable information will not be collected.

The anonymous identifier beacon keys remain on a person's phone unless that person reports a positive COVID-19 diagnosis through the app. At that point, the phone uploads the last 14 days of proximate contact data to a server, which sends automated alerts to the individuals whose beacon keys are in the dataset. The alert provides recipients with public health information and what actions to take without revealing the identity of the infected person.

Considerations for Implementation

Discussion of U.S. digital contact tracing has identified a number of challenges related to its use, including Bluetooth limitations, app effectiveness versus personal privacy, interoperability, and coverage. Each poses a different challenge to effective use of digital tracing capabilities.

Bluetooth Limitations

The Bluetooth signal strength and attenuation are variable and affected by numerous factors. Distance between smartphones, smartphone type, and object interference affect signal strength, which will be stronger when a smartphone is carried by hand and weaker from the bottom of a purse. Signal variation will make distance sensitivity calibration difficult, affecting the accuracy of the app. Observers have noted that if the calibration is too sensitive, there would be a risk of false positives, but if it is not sensitive enough, some interactions would go undetected.

App Effectiveness Versus Personal Privacy

Bluetooth data cannot provide the location of possible contacts, only that two users have been proximate. Global Positioning System (GPS) data, and to a lesser extent cell tower signal and Wi-Fi data, can provide location information. Apps collecting both Bluetooth and location data provide greater detail to health officials than apps using only Bluetooth tracking, which may better support manual contact tracing efforts by identifying where exposure may have occurred. Apple and Google, though, have explicitly banned the collection of location data by apps built using their protocol to protect individual privacy.

State public health officials will need to decide to either use a Bluetooth-only app that will only identify encounters or use another app that will identify encounters and collect more detailed location data. They will also need to determine whether to make the use of digital contact tracing apps mandatory. Privacy advocates have raised concerns surrounding apps using location data, fearing the data may be used for punitive purposes, such as individual quarantine enforcement, or used for purposes unrelated to fighting the pandemic, such as law enforcement.

Interoperability

As of May 20, 2020, Apple and Google have reported that 22 countries across 5 continents and many U.S. states have decided to base their apps on its protocol. As noted earlier, though, some countries and U.S. states developed their digital contact tracing apps before Apple and Google made their announcement. Since Apple and Google disallow the collection of location data in apps using their protocol, the state apps already in use, and any new apps that use location data, will not be interoperable with those using the Apple-Google protocol. The inability to exchange data among some proximate app users will impact the effectiveness of digital contact tracing efforts.

Coverage: Public Attitudes and Tech Availability

Many epidemiologists have stated that apps will be effective in halting the spread of COVID-19 nationwide if between 60% and 80% of the population downloads and uses them. However, it may not be possible to reach even the low end of this estimate. A recent Washington Post-University of Maryland poll found that nearly 60% of Americans would be either unable or unwilling to use a digital contact tracing smartphone app. Differences in state digital contact tracing requirements and uneven adoption across states may further complicate efforts to reach the required number of users nationwide.

U.S. smartphone ownership rates will affect the ability to reach the estimated number threshold needed for effective digital contact tracing. The Pew Research Center found that in 2019, 81% of Americans had a smartphone, but that figure is lower for the elderly and those making less than $50,000. Those without smartphones will not benefit from public health interventions enabled by digital tracing apps.

Related Legislative Proposals

As of May 22, 2020, three bills have been introduced that address privacy issues related to digital contact tracing apps, one proposal from the Senate and a second proposal that has been introduced in both the House and the Senate:

- The Public Health Emergency Privacy Act (H.R. 6866, S. 3749) was introduced in the House by Representative Anna Eshoo on May 14, 2020, and referred to the Committee on Energy and Commerce the same day. The bill was introduced in the Senate by Senator Richard Blumenthal the same day and referred to the Committee on Health, Education, Labor, and Pensions.

- The COVID-19 Consumer Data Protection Act of 2020 (S. 3663) was introduced in the Senate by Senator Roger Wicker on May 7, 2020, and referred to the Committee on Commerce, Science, and Transportation the same day. A House version has not been introduced.

The three bills aimed at securing the data collected by digital contact tracing apps differ significantly in their approaches, such as:

- how and to what extent the legislation would ensure government transparency and consumer privacy;
- the scope of entities covered (private, or public and private);
- whether to preempt state laws that might require more robust consumer protections; and
- whether to provide a private right of action to individuals against companies if their data is used in an unauthorized manner.

Patricia Moloney Figliola, Specialist in Internet and Telecommunications Policy

IF11559

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.