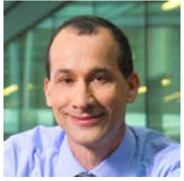
IAPP Privacy Perspectives:

Protecting privacy on COVID-19 surveillance apps

May 8, 2020



Paul Schwartz

Right now, there are signs that the curve of new COVID-19 cases in the United States is reaching a plateau, if not yet declining. We also have at least rough agreement among public health experts about the nation's necessary next steps. The need is for a dramatic expansion of testing, a ramping up of the ranks of public health workers to trace contacts, and interoperable digital platforms that permit real-time analysis of COVID-19 outbreaks.

As part of this effort, there is a frequently envisioned role for a COVID-19 cellphone surveillance app to further the plan for contact tracing. The app is to provide a technological solution to help identify parties with whom a COVID-19-infected person had contact. A COVID-19 app does so by drawing on information about the location of the mobile phone and its proximity to other devices.

The apps are here now and their impact on privacy and civil liberties will depend heavily on their design and the conditions for their use. Different kinds of contact tracing apps are already in place in Australia, Austria, China, Poland, Singapore, South Korea, Switzerland and Taiwan. In other countries, such as France, Germany and the United Kingdom, these apps are in development. The U.K. is about to begin testing its system for contact tracing on the Isle of Wight. In the U.S., North Dakota and Utah currently offer COVID-19 tracking apps to their residents, and one is in development in Hawaii.

What is the potentially positive role of a COVID-19 tracking app?

As a report from the Bloomberg School for Public Health at John Hopkins has pointed out, this technology "can act as force multiplier" for contact tracing. It would do so by exponentially increasing the capacity of the public health workforce, a body whose numbers have been drastically reduced by funding cuts over the past decades.

Interestingly, just as COVID-19 is a pandemic, the debate about the use and development of COVID-19 tracking apps is taking place worldwide. The most vibrant international debate about technology-assisted contact tracing is occurring in the European Union. While a columnist in a leading German newspaper, the Frankfurt Allgemeine Zeitung, dismissed this policy discussion as a “Nerd-Gezänk” (Nerd-Argument), the stakes are high, and the U.S. stands to learn from it.

The specific quarrel that the German paper pointed to concerned two competing app projects. Both have cumbersome acronyms: In one corner is the PEPP-PT, and in the other, the DP3T. The PEPP-PT program was to be the leading European initiative for a COVID-19 app but has run into a significant controversy around two topics. The first is whether data from the app should be stored in a centralized database or in a decentralized fashion. The second is whether the development of this project is transparent enough.

The DP3T, which is already in use in Austria and Switzerland, stores information in a decentralized fashion. Many data scientists view this approach as providing greater data security, and the European Parliament has pointed to it as its preferred solution. Thus, the PEPP-PT has run into a headwind to the extent that it is viewed as favoring centralized data storage.

As for the transparency issue, it is crucial because public use of these apps ultimately depends on the extent of trust in them. The PEPP-PT project has been attacked for its perceived lack of openness, and some scientists and their institutions have resigned from the project.

A wild card in this policy landscape is the app now in development by Google and Apple. Their joint contact tracing tool will soon be available worldwide and favors decentralized data storage. The devil is in the details, however, and the U.S., unfortunately, lacks an independent data protection oversight authority to evaluate this project.

Moreover, the Trump administration is proceeding with a characteristic lack of transparency in its COVID-19 response, including in its development of a tool, reportedly called “HHS Protect Now,” to allow the Department of Health and Human Services to integrate datasets from the public and private sectors to track the spread of the pandemic. Palantir, a private sector analytics company, is said to have received the federal contract to build this platform.

Fortunately, there is already agreement on both sides of the Atlantic about best practices in the area of COVID-19 tracking apps. Drawing on recommendations from the European Data Protection Board, EU’s national data protection commissioners, American Civil Liberties Union and Electronic Frontier Foundation, one can identify a core set of best practices:

- The use of a COVID-19 tracing app must be a voluntary choice by the individual.
- The app’s design must preserve privacy whenever possible in its use of identifiers and its other aspects.
- Only the minimum amount of information should be collected to support the targeted public health function of combating COVID-19.
- Development of COVID-19 tracing apps must be done in an accountable fashion with publicly available source code, an ability to audit and update the app, and documentation of the technology’s privacy impact.
- Data security, including state-of-the-art encryption, must be used to protect all data, whether in storage or in motion.

- Protections must be in place against “mission creep,” including setting an end to the program once the current crisis ends, or, as the ACLU puts it, developing “an exit strategy” for the app’s use.

Two final observations are necessary.

First, the COVID-19 app cannot be viewed as a silver bullet. Much is unknown about how the virus spreads, and public health officials will likely have to revise their views on the kinds of proximity relevant to COVID-19 transmission and provide advice on necessary changes to apps that are in use. Moreover, any technology, including Bluetooth tracking, will have imperfections in its ability to track contacts. A frequently cited example is Bluetooth’s inability to determine whether people in close proximity are separated by a wall, as is the case for two residents in an apartment building, or are seated in restaurant tables near each other. The two situations present far different risks for transmission.

Second, a COVID-19 app can only be helpful as a part of a larger governmental response to the pandemic. Sadly, such a national strategy, including robust testing programs and ramped up contact tracing by public health workers, is not yet in place. In taking the next steps in our country’s response to the pandemic, we cannot count on proximity apps as a magical solution, but only as a part of a comprehensive national approach.

https://iapp.org/news/a/protecting-privacy-on-covid-surveillance-apps/