The Heritage Foundation

ISSUE BRIEF
No. 5065 | APRIL 30, 2020
DOUGLAS AND SARAH ALLISON CENTER FOR FOREIGN POLICY

The Apple–Google Partnership to Fight COVID-19: Understanding the Promises and Perils of Digital Contact Tracing

Klon Kitchen

KEY TAKEAWAYS

Apple and Google have announced that their mobile devices—99 percent of the U.S. market—will soon support voluntary digital contact tracing in response to COVID-19.

Industry and government should adopt a set of standards that maximize the utility of digital-contact-tracing apps while assuaging legitimate privacy concerns.

These apps should collect the minimum amount of data necessary, and ensure that data are anonymous, encrypted, and unavailable for use by law enforcement.

On April 10, Apple and Google announced that their mobile devices will soon support voluntary digital contact tracing in response to the COVID-19 pandemic.[1] This support from the two companies that comprise 99 percent of the U.S. mobile phone market is significant because it promises to increase the scale and speed of contact tracing, and because it provokes questions about security and privacy. It is essential, then, to have a firm grasp of the details and of the facts in order to navigate the promises and perils of digital contact tracing.

What Is Contact Tracing?

According to the Centers for Disease Control and Prevention (CDC), contact tracing is "a core disease control measure employed by local and state health department personnel" where they "work with

a patient to help them [sic] recall everyone with whom they [sic] have had close contact during the timeframe while they [sic] may have been infectious" and then "warn those exposed individuals (contacts) of their potential exposure."[2]

Is Contact Tracing Necessary?

Yes, contact tracing is necessary for understanding and controlling the spread of COVID-19. Contact tracing is one public health tactic that has been a fundamental element of epidemiological response for decades. Whereas testing allows health officials to understand where a disease has been, contact tracing allows them to predict where it will go, and to slow down that spread using a wide range of transmission mitigation actions, most often encouraging those who may have come in contact with an infected person to seek testing.

To be clear: manual contact tracing has been a part of every successful pandemic response in modern history and it is described by virtually every public health official and agency, including the Trump Administration, as a prerequisite for safely managing the COVID-19 challenge and for quickly and safely re-opening the areas of the U.S. that have been most affected by the virus.

The current debate is not over whether to use contact tracing. It is over how best to introduce digital technologies to accomplish contact tracing in ways that maintain, or enhance, individual privacy. A path forward exists that, if implemented correctly, will safeguard privacy.

How Does Contact Tracing Work?

Contact tracing is typically conducted by specially trained individuals who interview the infected and who find and inform their contacts of potential exposure. If a contact is infected, his or her contacts will be found as well, with the process continuing until everyone who has been exposed is found, and then potentially quarantined or isolated—helping to stop continued spread of the virus. Contact data are also entered into public health databases and used for models that inform pandemic policy and planning.

The CDC says that contact investigators should be trained to understand patient confidentiality, key medical terms and principles, crisis counseling, and have key cultural competencies.[3] Current staffing levels are not sufficient to meet the need for contact tracing on a wide scale during the current pandemic, so government and public health officials are adding staff and

volunteers. Even when enlisting volunteers, public health officials often struggle to conduct contact tracing at the speed and scale of transmission, and it will require significantly more investigators to keep up with COVID-19 using this method.

Dr. Hugh Montgomery, professor of intensive care medicine at University College London, makes the scale of the COVID-19 challenge clear:

> Normal flu, if I get that, I'm going to infect on average, about 1.3, 1.4 people—if there was such a division. And if those 1.3, 1.4 people gave it to the next lot, that's the second time it gets passed on. By the time that happened 10 times, I've been responsible for about 14 cases of flu. This coronavirus is very, very infectious, so every person passes to three [and if] each of those three passes to three, and that happens at 10 layers, I have been responsible for infecting 59,000 people.[4]

What Are Apple and Google Building and How Will It Work?

Considering the scale and speed challenges, and because they have a stake in the United States' economic recovery, Apple and Google are deploying an application programming interface (API) that will allow developers to build contact tracing apps that work on Apple's iOS and Google's Android mobile operating systems. This API shapes how these apps collect and use information for contact tracing.

Based on available information, Apple and Google appear to be prioritizing privacy within the API. Here is an example of how the companies say that digital contact tracing will work using the fictional example of "John" and "Abigail":

- On Monday, John and Abigail are standing at a bus stop waiting for a bus. While waiting there, their phones exchange unique but anonymous identification codes via their phones' Bluetooth capability. No personally identifying information (PII) or location data are shared, and all data stay on their phones by default.

- A few days later, Abigail is diagnosed with the coronavirus and opts to share this diagnosis with an app developed by a local public health authority. With her consent, Abigail's phone uploads all the anonymous identification codes of individuals she has been near over the past 14 days.

- Meanwhile, John's phone is regularly downloading a list of anonymous identification codes associated with people who have chosen to share their positive coronavirus diagnosis and compare these codes with those John has been near.

- After Abigail chooses to share her diagnosis and allows that information to be shared with others, John receives a notification that he has been in contact with someone who has tested positive as well as added suggestions on what to do next. John is not told who was infected or where and when the contact with this person occurred—only that his exposure was sometime in the past two weeks.

The entire process is voluntary. Users must actively opt in to download the app, to share their COVID-19 diagnosis, and to have that diagnosis shared with others. They can also stop taking part at any time.

Apple and Google say that this API will eventually be folded into their base mobile operating systems, but that this will not significantly change how digital contact tracing works or the data that are used.

Anecdotally, even the American Civil Liberties Union (ACLU) believes that Apple and Google are demonstrating serious concerns about privacy. The ACLU's surveillance and cybersecurity counsel issued a statement that,

> [t]o their credit, Apple and Google have announced an approach that appears to mitigate the worst privacy and centralization risks, but there is still room for improvement. We will remain vigilant moving forward to make sure any contact tracing app remains voluntary and decentralized, and used only for public health purposes and only for the duration of this pandemic.[5]

What Kind of Information Will Be Shared with Technology Companies?

The API does not collect any information beyond a user's anonymous identification codes and the codes of those with whom they have been in close proximity. Even this information must be voluntarily shared. Again, no location data, Internet activity, or PII is necessarily collected or shared. If app developers want more information from a user, they will have to explicitly request that information and the user will have to willingly provide it.

That is not to say that this is the only information that technology companies have. Apple, Google, and virtually all other app developers routinely collect significant volumes of data, including a user's contacts, location,

Internet viewing habits, and online shopping history. They will still have this information regardless of whether a user chooses to take part in digital contact tracing, but they will not have *more* information if a user takes part.

In summary: As described by Apple and Google, a person's participation in digital contact tracing does not appreciably increase or decrease their exposure to broader data collection by technology companies.

What Kind of Information Will Be Shared with the Government?

The proposed API will allow public health organizations to integrate the voluntarily provided, anonymous diagnosis, and contact information into their existing tracing and modeling programs. This allows them to have greater insight into the pandemic, and is similar to traditionally collected contact tracing, only it creates uniform reporting standards, allows much of the work to be automated and faster, and supports a higher level of individual privacy through encryption and anonymization. These databases and models are shared with local, state, and federal policymakers to inform their management of the crisis.

While the proposed API will not give government officials at any level the ability to identify users, these officials will retain their subpoena and warrant authorities unless they are explicitly constrained by law. This means that the government could theoretically require technology companies to provide correlating information that could be combined with digital contact tracing data to identify individuals. Although, it must be said, Apple and Google appear to be designing the API to have minimal law enforcement utility. This is because such correlating activity would be a self-defeating strategy, as companies could disclose these requests as a part of their routine "transparency" reporting, likely causing users to abandon digital contact-tracing applications in droves at the time when they are most needed.

Are Other Entities Engaging in Digital Contract Tracing?

Yes. The governments of China, Singapore, and Taiwan have successfully used digital contact tracing. It is also being deployed in Australia and actively considered by several other countries, including Germany and other members of the European Union. It must be noted, however, that there is a broad range of privacy expectations and approaches among these examples.

How Can Privacy Risks and Government Overreach Be Minimized?

Expanding the scale and speed of contact tracing will serve both individual and public health interests. Furthermore, private-sector efforts to innovate and to service critical public needs should be lauded and encouraged. That said, distrust of "big tech" and of "big government" could decisively undermine the adoption and efficacy of Apple's and Google's digital contact tracing plans. Legislation is not needed for these plans to go forward, but in an effort to calm public fears, some are calling for new laws that would constrain industry and government. This is a suboptimal approach because it risks creating potentially unconstitutional constraints on private companies and on governments at the local, state, and federal level. Instead, industry and government should adopt a set of robust privacy standards aimed at maximizing the utility of digital contact tracing while also assuaging the most prominent public concerns about this activity.

These robust privacy standards and commitments should include the following:

- Digital contact tracing data will always be anonymized, and tracing apps will only collect the minimum data needed to inform individuals of their risk of COVID-19 infection and to enable general pandemic tracking and response by public health and government officials.

- Digital contact tracing data will be encrypted at rest and in transit.

- Digital contact tracing data will not be sold by technology companies or used for product development, advertising, or any other commercial enterprise.

- Digital contact tracing data will not be used by local, state, or federal law enforcement or intelligence departments or agencies.

- Digital contact tracing data will be deleted completely from public and private servers within 21 days of collection (one week after the utility of the data expires in the case of COVID-19).

- Individual use of digital contact tracing apps may not be mandated by local, state, or federal government.

- Technology companies may not be required by local, state, or federal government to collect user PII through digital contact tracing apps.

- Public health agencies should prepare now to use the tools being created and their use should comply with the above recommendations for private companies.

Klon Kitchen is Senior Research Fellow for Technology, National Security, and Science Policy in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

Endnote

1. News release, "Apple and Google Partner on COVID-19 Contact Tracing Technology," Apple, https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ (accessed April 27, 2020).
2. Centers for Disease Control and Prevention, "Contact Tracing: Part of a Multipronged Approach to Fight the COVID-19 Pandemic," https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html (accessed April 27, 2020).
3. Ibid.
4. Chiara Giordano, "Coronavirus Is Very, Very Infectious: Doctor Explains How One Person Can Infect 59,000 Others," The Independent, March 2020, https://www.independent.co.uk/news/health/coronavirus-infections-symptoms-flu-doctor-dispatches-a9419146.html (accessed April 27, 2020).
5. News release, "ACLU Comment on Apple/Google COVID-19 Contact Tracing Effort," American Civil Liberties Union, https://www.aclu.org/press-releases/aclu-comment-applegoogle-covid-19-contact-tracing-effort (accessed April 27, 2020).