GlobalResearch
Center for Research on Globalization

Apple and Google Announced a Coronavirus Tracking System. How Worried Should We be?

A well-designed tool could offer public health benefit, but a poorly designed one could pose unnecessary and significant risks to privacy, civil rights, and civil liberties.

By Jennifer Stisa Granick
Global Research, April 20, 2020
ACLU 16 April 2020

Region: USA
Theme: Intelligence, Police State & Civil Rights, Science and Medicine

Apple and Google last week announced a joint contact tracing effort that would use Bluetooth technology to help alert people who have been in close proximity to someone who tested positive for COVID-19. Similar proposals have been put forward by an MIT-associated effort called PACT as well as by multiple European groups.

These proposals differ from the traditional public health technique of "contact tracing" to try to stop the spread of a disease. In place of human interviewers, they would use location or proximity data generated by mobile phones to contact people who may have been exposed.

While some of these systems could offer public health benefits, they may also cause significant risks to privacy, civil rights, and civil liberties. If such systems are to work, there must be widespread, free, and quick testing available. The systems must also be widely adopted, but that will not happen if people do not trust them. For there to be trust, the tool must protect privacy, be voluntary, and store data on an individual's device rather than in a centralized repository.

A well-designed tool would give people actionable medical information while also protecting privacy and giving users control, but a poorly designed one could pose unnecessary and significant risks to privacy, civil rights, and civil liberties. To help distinguish between the two, the ACLU is publishing a set of technology principlesagainst which developers, the public, and policymakers can judge any contact tracing apps and protocols.

Technology principles that embed privacy by design are one important type of protection. There still need to be strict policies to mitigate against overreach and abuse. These policies, at a minimum, should include:

- Voluntariness — Whenever possible, a person testing positive must consent to any data sharing by the app. The decision to use a tracking app should be voluntary and uncoerced. Installation, use, or reporting must not be a precondition for returning to work or school, for example.
- Use Limitations — The data should not be used for purposes other than public health — not for advertising and especially not for any punitive or law enforcement purposes.
- Minimization — Policies must be in place to ensure that only necessary information is collected and to prohibit any data sharing with anyone outside of

the public health effort.

- Data Destruction — Both the technology and related policies and procedures should ensure deletion of data when there is no longer a need to hold it.
- Transparency — If the government obtains any data, it must be fully transparent about what data it is acquiring, from where, and how it is using that data.
- No Mission Creep – Policies must be in place to ensure tracking does not outlive the effort against COVID-19.

These policies, at a minimum, must be in place to ensure that any tracking app will be effective and will accord with civil liberties and human rights.

The Apple/Google proposal, for instance, offers a strong start when measured against these technology principles. Rather than track sensitive location histories, the Apple/Google protocol aims to use Bluetooth technology to record one phone's proximity to another. Then, if a person tests positive, those logs can be used to notify people who were within Bluetooth range and refer them for testing, recommend self-isolation, or encourage treatment if any exists. Like the similar proposals, it relies on Bluetooth because the location data our cell phones generate is not accurate enoughfor contact tracing.

Like location histories, however, proximity records can be highly revealing because they expose who we spend time with. To their credit, the Apple/Google developers have considered that privacy problem. Rather than identify the people who own the phones, apps based on the protocol would use identifiers that cannot easily be traced back to phone owners.

As of this writing, the Apple/Google protocol could better address certain important privacy-related questions, however. For example, how does the tool define an epidemiologically relevant "contact"? The public needs to know if it is a good technological approximation of what public health professionals believe is a concern. Otherwise, the tool could be collecting far more personal information than is warranted by the crisis or could cause too many false alarms. And if there is indeed a plan to terminate the program at the conclusion of the pandemic, what criteria are the companies using to indicate when to press the built-in self-destruct button?

Another issue is whether phone users control when to submit their proximity logs for publication to the exposure database. These decisions should be made by the phone user. There may be good reasons why people do not want to upload all their data. User control can help to reduce false positives, for example if a user knows that identified contacts during that time were inaccurate (because they were in a car or wearing protective gear). It would also encourage people whose records include particularly sensitive contact information to at least volunteer the non-sensitive part of their records rather than fail to participate completely.

Also, when users share their proximity logs, what will they reveal? Right now, under the Apple/Google proposal, an infected user publicly shares a set of keys. Each key provides 24 hours of linkable data — a length of time that threatens the promised anonymity of the system. It is too easy to re-identify someone from 24 hours of data and the current proposal makes it impossible for the user to redact selected times during the day. There are other options that would ensure that identifiers published in the exposure database are as difficult as possible to connect to a person's name or identity.

Voluntariness is particularly important. A critical mass of people will need to use a contact tracing app for it to be an effective public health mechanism, but some proposals to obtain that level of adoption have been coercive and scary. This is the wrong approach. When people feel that their phones are antagonistic rather than helpful, they will just turn location functions off or turn their phones off entirely. Others could simply leave their phone at home or acquire and register a second, dummy phone that is not their primary device with which they leave home. Good public health measures will leverage people's own incentives to report disease, respond to warnings, and help stop the virus's spread.

In the coming weeks and months, we are going to see a push to reopen the economy — an effort that will rely heavily on public health measures that include contact tracing. Bluetooth proximity tracking may be tried as a part of such efforts, though we don't know how practical it will prove in real-world deployments. But privacy-by-design principles and the policy safeguards outlined here must be core to that effort if we are to benefit from a proximity tracking tool that can give people actionable medical information while also protecting privacy and giving users control.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Jennifer Stisa Granick, Surveillance and Cybersecurity Counsel

---