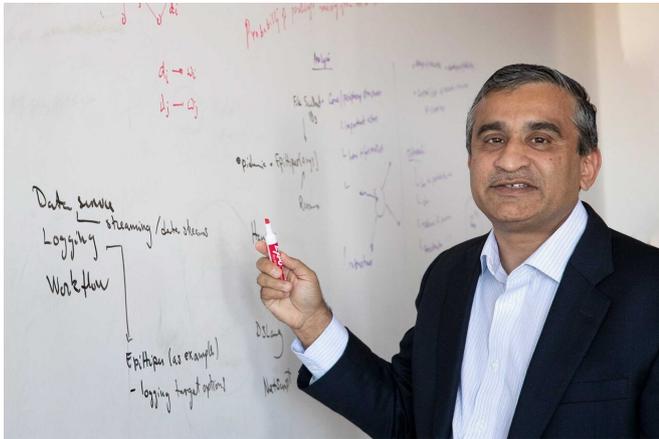


# Everything you need to know about your smartphone's new COVID-19 tracker

23 April 2020



UVA computer science professor Madhav Marathe calls the partnership between tech giants Apple and Google a “laudable initiative.” Credit: Dan Addison, University Communications

Apparently a global pandemic makes strange bedfellows.

That was one of the first things to come to mind following the recent announcement that Google and Apple would work together to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the coronavirus by tracking the movements and interactions of users.

All of this prompts another question: Will the advent of the new smartphone software put personal privacy at risk?

For the lowdown on how the [technological advances](#) on our iPhone and Android devices—scheduled to roll out in mid-May—will work, UVA Today turned to computer science professor Madhav Marathe, one of the leaders of the University of Virginia's Biocomplexity Institute, who replied to questions via email.

**Q. What was your reaction when you saw that Apple and Google would be collaborating on this project?**

A. I think this is a laudable initiative. Both companies have significant depths in computing and understand the issues related to privacy very well. They also have control at the [operating system] level that allows them to undertake the development of projects that employ the complete software stack, thus making the solution efficient, scalable and useable.

Other groups, including the TCN consortium, CoEpi and NOVID are also working on similar questions.

**Q. For those who may not be technologically inclined, can you explain in very simple terms what the companies are doing with this new smartphone software and how it will work?**

A. In very simple terms, these companies are developing an app that alerts an individual who comes in close proximity of another individual who later tests COVID-19 positive. This works only when both the individuals have the app. It is done in four simple steps: one, users download the apps; two, then the users come within certain distances of each other, they exchange their encrypted keys (they are generated frequently and cannot be identified with a device directly); three, when an individual with the app falls sick and gives consent, their own keys get uploaded to the cloud; and four, all apps download these keys every so often and see if the keys match one of the keys that they had stored. Keys are generated randomly and frequently.

So tracking a user's movement is not easy. It also does not store the interaction explicitly in the cloud. The cloud only has keys of the infected users and that, too, in an encrypted form. So in summary, an individual can know that someone who was in close proximity at some time was infected. It does not

reveal who the person was, when the person might have come in physical proximity and where this encounter might have happened. In this sense, it preserves three important elements of privacy: "who?," "when?" and "where?"

Of course, correlation attacks are still possible, using other cameras or other tracking technology to correlate users with the keys generated. However, those attacks would be difficult to execute, especially on a large scale.

**Q. The companies say that "privacy, transparency, and consent are of utmost importance in this effort." In your opinion, should the public feel confident in this?**

A. Although experts have pointed to a few potential security flaws, I believe they are not as serious. The primary concern is locational information, and the experts point to correlational attacks to identify users at certain locations. But as other articles have pointed out, while this is certainly possible, there are other ways to track a user and that this can only be done for a user that tests COVID-19 positive.

This does not mean that the proposed solution is 100% privacy-preserving. It, however, does mean that it is unlikely that one can do this at a large enough scale due to proximity constraint and the fact that only keys pertaining to people who were proximal for long enough period can potentially be identified in this way. (See this Wired article for additional discussion.)

**Q. From purely a technological standpoint, what do you think of this idea?**

A. I believe this is a good idea to explore. Making an app completely secure is quite unlikely; I believe this app strives to strike a good balance between public health needs and personal privacy. Furthermore, once the COVID-19 pandemic recedes, one can easily disable the app.

**Q. Do you think the software will be helpful in combatting COVID-19? Aside from possible privacy infringements, are there any other dangers?**

A. The usefulness of the app will depend on the participation by the public (they need to download the app). This implies that a large section of the society might be completely missed either due to technological challenges or due to concerns related to [personal privacy](#).

Second, individuals who have a confirmed COVID-19 case have to agree to upload their keys to the cloud. They may or may not choose to do this.

Finally, individuals who receive the information, may or may not act on the information.

In spite of these limitations, such an app can potentially be useful; its efficacy can only be tested after it is deployed.

**Q. Are there any other ways—or better ways—Apple and Google could be helping during this crisis? Anything you'd like to see them try and do?**

A. There are number of other ways Google and Apple can help during crisis. One is providing mobility related data; both companies have already taken important steps in this direction. (See Apple's reports and Google's.)

Second, they can provide computing services, which again Google has begun providing; see the COVID-19 High Performance Computing Consortium. Finally, the companies can develop innovative products as they pertain to providing information about health care resources and information accessible from Google Search trends.

**Q. Anything else you'd like to add?**

A. Contact tracing is an important tool in the fight against COVID-19. Apps such as the ones Google and Apple are developing is a step in the right direction.

Importantly, as a society, we need to have a serious debate that is about balancing privacy and public health during a crisis like this. Laws need to be enacted now so that [people in] future pandemics can benefit, rather than waiting for an

event such as COVID-19 to happen.

In the end, the success of the apps depends a lot on user participation. Each country has adopted a different balance between [privacy](#) and public health. It is time to act now.

Provided by University of Virginia

APA citation: Everything you need to know about your smartphone's new COVID-19 tracker (2020, April 23) retrieved 2 July 2022 from <https://techxplore.com/news/2020-04-smartphone-covid-tracker.html>

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.*