

Do COVID-19 apps protect your privacy?

9 June 2020, by Jodi Heckel



Information sciences professor Masooda Bashir and doctoral student Tanusree Sharma analyzed 50 mobile apps that track the spread of COVID-19 and their privacy protections. Bashir studies information technology, human psychology and society, including how privacy, security and trust intersect with information systems. Credit: Masooda Bashir

Mobile apps are helping track the spread of COVID-19 to contain the outbreak, but the apps also raise concerns about personal privacy.

Information sciences professor Masooda Bashir and doctoral student Tanusree Sharma at the University of Illinois at Urbana-Champaign analyzed 50 COVID-19-related apps available in the Google Play store for their access to users' personal data and their privacy protections. Bashir and Sharma found that most of the apps required access to users' [personal data](#), but only a handful indicated the data would be anonymous, encrypted and secured.

They report their findings in the journal *Nature Medicine*.

"What is disconcerting is that these apps are continuously collecting and processing highly sensitive and personally identifiable information,

such as [health information](#), location and direct identifiers (e.g., name, age, email address and voter/national identification)," they wrote in the journal article. "Governments' use of such tracking technology—and the possibilities for how they might use it after the pandemic—is chilling to many. Notably, surveillance mapping through apps will allow governments to identify people's travel paths and their entire social networks."

The functionalities of the COVID-related apps developed around the world include live maps and updates of confirmed cases, real-time location-based alerts, systems for monitoring home isolation and quarantine, direct reporting to the government of symptoms and education about COVID-19. Some also offer monitoring of vital signs, virtual medical consultations and community-driven contact tracing.

Of the 50 apps the researchers evaluated, 30 require users' permission to access data from their [mobile devices](#) such as contacts, photos, media, files, location data, the camera, the device's ID, call information, Wi-Fi connection, microphone, network access, the Google service configuration and the ability to change network connectivity and audio settings. Some of the apps state they will collect users' age, [email address](#), phone number and postal code; the device's location, unique identifiers, mobile IP address and operating system; and the types of browsers used on the device.

Only 16 of the apps indicated such data will be anonymous, encrypted, secured and reported only in aggregate form.

Of the apps sampled, 20 were issued by governments, health ministries and other such official sources. It is not clear if the data collected by the apps is protected by laws such as the Health Insurance Portability and Accountability Act, and the U.S. doesn't have a structured privacy framework in place as Europe does, the researchers wrote.

They acknowledged that mass surveillance measures may be necessary to contain the spread of the virus.

"Health care providers must absolutely use whatever means are available to save lives and confine the spread of the virus," they wrote. "But it is up to the rest, especially those in the field of information privacy and security, to ask the questions needed to protect the right to privacy."

More information: Tanusree Sharma et al, Use of apps in the COVID-19 response and the loss of privacy protection, *Nature Medicine* (2020). DOI: [10.1038/s41591-020-0928-y](https://doi.org/10.1038/s41591-020-0928-y)

Provided by University of Illinois at Urbana-Champaign

APA citation: Do COVID-19 apps protect your privacy? (2020, June 9) retrieved 28 November 2021 from <https://techxplore.com/news/2020-06-covid-apps-privacy.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.