COVID-19 contact tracing apps: Eight privacy questions governments should ask

April 2 2020, by Caroline Brogan

Credit: CC0 Public Domain

As part of their efforts to slow the outbreak of coronavirus, governments, research institutions and industry are developing contact tracing apps to record interactions between people. The apps warn users if one of the people they have been recorded as being in contact with is later diagnosed with COVID-19 so they can take appropriate steps like

self-isolation.

Such apps could prove useful in avoiding long-term confinement measures. However they collect sensitive information like location data, Bluetooth-enabled proximity information, and whether individuals are infected.

Now, a new white paper by Imperial College London's Dr. Yves-Alexandre de Montjoye has outlined eight questions that should be asked to understand how protective of privacy an app is.

Dr. de Montjoye, of Imperial's Department of Computing, said: "We need to do everything we can to help slow the outbreak. Contact tracing requires handling very sensitive data at scale, and solid and proven techniques exist to help us do it while protecting our fundamental right to privacy. We cannot afford to not use them.

"Our questions are intended for governments and citizens to help evaluate the privacy of apps. They could also for app developers when planning and evaluating their work."

The questions were developed by a team including Imperial Ph.D. students Florimond Houssiau, Andrea Gadotti, and ENS Lyon's Florent Guepin.

The questions

1. How do you limit personal data gathered by the app developers?

Dr. de Montjoye (YDM): "Large-scale collection of personal data can quickly lead to mass surveillance. We should ask how much data the app

gathers—like the whole disease trajectory and real-life social network of infected users."

2. How do you protect the anonymity of every user?

YDM: "Special measures should be put in place to limit the risk that users can be re-identified by app developers, other users, or external parties. Because location traces are unique, they might easily be linked back to a person."

3. Does the app reveal to its developers the identity of users who are at risk?

YDM: "The goal of contact tracing is to warn people who are at risk, so there's no need for app developers to know who these people are."

4. Could the app be used by users to learn who is infected or at risk, even in their social circle?

YDM: "Personal health data is very sensitive. Digital contact tracing should warn those who are at risk without revealing who might have infected them."

5. Does the app allow users to learn any personal information about other users?

YDM: "Having access to small amounts of information could help users identify who is infected, so apps shouldn't disclose information on a user's location or social networks to other users."

6. Could external parties exploit the app to track users

or find out who's infected?

YDM: "Apps should consider the risk of external adversaries, including well-resourced ones. External entities could install Bluetooth trackers to cover a city, or install malicious code on phones, and record the identifiers that they observe in specific locations. This can be avoided by regularly changing and re-anonymising identifiers like location data."

7. Do you put in place additional measures to protect the personal data of infected and at-risk users?

YDM: "The app design may require revealing more personal information about users who are infected or exposed, but these are often the people who are more vulnerable and at risk. It's important to consider what additional measures can be taken to protect their information."

8. How can users verify that the system does what it says?

YDM: "Large-scale contact tracing is too sensitive an issue to rely on blind trust. Technical measures should be used to guarantee public scrutiny on the functioning of the app. Transparency of the system (app code, protocol, what is being broadcast, etc) is fundamental to guarantee privacy. This requires that the app be open source and app versions distributed on mobile app stores be verifiable, enabling developers to confirm that they're running the public, auditable code."

Privacy a 'crucial component' going forward

Contact tracing apps are being developed around the world and some are already available. If they are proven useful, governments, health

authorities, and users will have to evaluate the different approaches and decide whether to adopt them. Privacy, say the researchers, is a crucial component in this decision.

Co-author Florimond Houssiau, also from Imperial's Department of Computing, said: "These questions are meant to be a starting point for an informed conversation on privacy in contact tracing apps."

The questions do not cover every potential vulnerability of contact tracing protocols, like security issues. Co-author Andrea Gadotti said: "Our questions focus on privacy, but the security side is equally important. This means, for example, encrypting the apps, evaluating how mobile malware could affect the app's behaviour, and assessing the resilience of the app developer servers against intrusion."

Provided by Imperial College London