

COVID-19 Tracing Applications & Privacy: Should Canadians Be Concerned?

When the federal government first announced in June the development of a COVID-19 app in Ontario, I was thrilled. To my surprise, however, many of my friends and family did not feel the same way. An application that could inform you of potential COVID-19 exposures, why was everyone so concerned? But after hearing the news of Iran's AC19 app, it became more clear.

On March 3, tens of millions of Iranian citizens received a mobile notification to download an app called 'AC19.' An application introduced by the Iranian Ministry of Health, promoted for its ability to self-diagnose and detect COVID-19 infections.

Once downloaded, individuals register using their mobile number. They are then prompted to give the app permission to send their precise location to the government's servers. The app then asks a series of YES or No questions regarding COVID-19 symptoms and requires individuals to provide their personal medical information. This information is then submitted for assessment.

Within seconds, the app provides a diagnosis, informing users if they are infected with COVID-19. Individuals diagnosed with severe symptoms are notified to go to the hospital.

Being one of the hardest-hit countries by the ongoing pandemic, this application provided many Iranian citizens with a promising solution to limit the spread of COVID-19. But after only six days of its introduction, the app was removed from the Google Play Store.

To date, no official reason has been provided. However, sources familiar with Play Store policies told ZDNet that Google most likely removed the app due to its "misleading claims, namely that it could detect and diagnose COVID-19 infections, something that is impossible through an app."

Nariman Gharib, an Iranian security researcher, told VICE News that he fears that the app's real-time tracking feature is being used for spying purposes. "Collecting location data is not a one-off thing," he states, highlighting Iran's alarming history of internet surveillance strategies.

In light of this news, I became concerned and paranoid. Were my privacy rights being violated by Canada's COVID Alert app? But after reviewing several academic studies and reading the work of various privacy commissioners, I realized that from a privacy perspective, the design of Iran and Canada's apps are night and day.

For starters, one significant difference is that Iran's AC19 app uses real-time tracking. The app uses GPS data for contact tracing, which can be used by the government for spying purposes.

In contrast, Canada's COVID Alert app uses Bluetooth connections. It does not track geo-location. Instead, the app utilizes Bluetooth to determine if an individual is near another person's phone. If two phones are nearby, a random code is exchanged and stored for two weeks.

If an individual were to test positive for COVID-19, they would be required to enter an anonymous one-time code into the application. After this code is entered, the application's central server will alert the random codes exchanged over the last two weeks, informing individuals anonymously that they may have been infected with COVID-19.

Secondly, the Iranian AC19 app, in addition to collecting a user's precise locations, collects sensitive private information. Security experts have discovered that the app sends information entered by the user, including their gender, name, height, and weight, back to the developer's server, which can be accessed by the government.

In comparison, Canada's Covid Alert app does not require personal information. When downloaded, individuals are only required to provide their phone number to register.

As mentioned previously, the COVID Alert app uses a random coding system to identify if two individuals are near one another. As such, the government does not rely on a user's personal information for identification. Instead, the government only collects a user's IP addresses. This IP address is not linked to any other information in the system, such as a user's phone number, and is randomly assigned to individuals once registered.

While it is apparent that the Canadian government has taken several precautionary steps to ensure anonymity, there is still a risk of re-identified. This risk is unlikely, but it is not impossible.

Daniel Therrien, a Privacy Commissioner, told CBC News that the Canadian government's claim of full anonymity is "misleading." For Therrien, anonymity "implies that there is no risk whatsoever that a person could be identified." However, although he agrees that there is a "very low risk that someone could be re-identified through the app, it isn't necessarily zero."

"Someone living in a remote area and only interacting with one or two other people could theoretically be identified by their neighbours if they received exposure notification alerts."

Of course, there is a risk of being re-identified through using the app, especially if an individual interacts with only a handful of people. This may cause individuals infected with COVID-19 to be identified and feel as though their privacy rights have been violated by the government.

This concerns me, but not enough to prevent me from downloading the COVID Alert app. As with anything, there is always a risk. While the issue of re-identification is a considerable privacy concern, given its very low risk, it should not impact one's choice to download the app. In turn, Canadians should not be concerned that the COVID Alert app will violate their privacy.