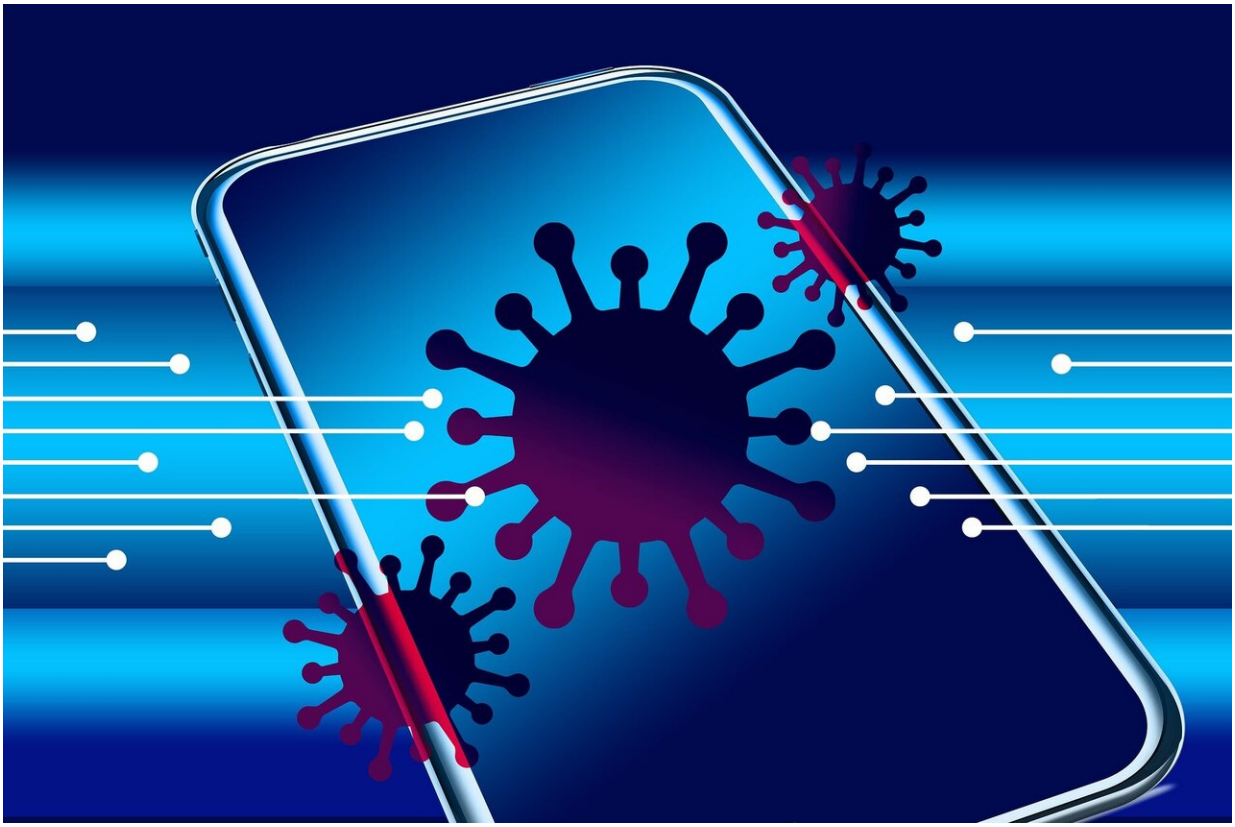
Researchers question Google Play component of COVID tracker apps

July 23 2020, by Catherine O'mahony



Credit: Pixabay/CC0 Public Domain

Prof. Doug Leith and Dr. Stephen Farrell at the School of Computer Science and Statistics have issued a new report concluding that user privacy is not protected adequately in COVID-19 tracking apps,

including the Irish COVID Tracker app.

The report examined the data transmitted to backend servers by the contact tracing apps deployed by health authorities in Germany, Italy, Switzerland, Austria, Denmark, Spain, Poland, Latvia, and Ireland with a view to evaluating user privacy.

The researchers described the Google Play Services component of these apps as "extremely troubling from a privacy viewpoint."

These apps consist of two separate components: a "client" app managed by the national public health authority and the Google/Apple Exposure Notification service, which—on Android devices—is part of Google Play Services.

They found that Google Play Services contacts Google servers roughly every 10-20 minutes, allowing fine-grained location tracking via IP address. In addition, Google Play also shares the phone IMEI, hardware serial number, SIM serial number, handset phone number and user email address with Google, together with fine-grained data on the apps running on the phone.

This level of intrusiveness, the researchers concluded, "seems incompatible with a recommendation for population-wide usage." Extending public governance to the full contact tracing ecosystem, not just of the health authority client app component, therefore seems to be urgently needed if public confidence is to be maintained, the report recommended.

The researchers noted they had informed Google of the findings and delayed publication to allow them to respond. Having collaborated with the Health Service Executive (HSE) as the Irish app was being developed, they also informed the HSE of their findings regarding the

COVIDTracker app and delayed publication to allow them time to respond, and similarly the developers of SmitteStop, Apturi COVID and ProteGO Safe.

Prof. Doug Leith, Chair of Computer Systems at Trinity College Dublin, said:

"We looked at the network traffic between Europe's Google/Apple API contact sharing apps and their backend servers. This is the first study of its type on the privacy of contact tracing apps actually deployed in the 'wild.' We found that the public health authority component of these apps generally shares little data and is quite private. However, on Android devices we found that the Google component of the apps is far from private and continuously shares a great deal of data with Google servers. This data includes the phone IMEI, hardware serial number, SIM serial number, handset phone number, the WiFi MAC address and approximate phone location. It's hard to imagine a more intrusive data collection setup and its obviously troubling. While there has been a great deal of public scrutiny of the public health authority component of these apps, including detailed Data Protection Impact Assessments and governance arrangements, there has been almost no public scrutiny of the Google/Apple component of the apps, and few governance measures put in place, despite the fact that it is the Google/Apple component which does most of the "heavy lifting" in the apps. We think that needs to change, and quickly, bearing in mind that these are public health apps sponsored by national governments and health authorities and have been installed by millions of people in good faith."

He continued, "We found that the Irish HSE app sets a type of 'supercookie' that allows connections made by the same phone to be linked together over time. None of the other European apps do this and we recommend it be removed. Unlike most other apps the HSE app also encourages people to opt in to collection of metrics. That's not

necessarily a problem in itself but these metrics include a mix of operational and health-related data and we recommend that these different types of data be kept securely separate from one another so that access can be separately controlled. When first installed the HSE app uses Google's SafetyNet service and so shares data with Google, including the phone hardware serial number. Most of the other European apps don't do this (the Polish app is the exception) and we recommend the HSE app should avoid it too. We also found that the Danish app fails to verify it is securely communicating with the correct server and so, for example, the act of uploading keys following a positive test phone call might be logged by an employer's network security devices. We recommend that they fix this and also that they make their app open source (only the Danish and Latvian apps are closed source). We also found the Latvian and Polish contact tracing apps make use of Google's Firebase service and so share data with Google. We recommend that this be discontinued."

Dr. Stephen Farrell, senior research fellow in the School of Computer Science and Statistics, said: "If there were a European league of COVID tracing apps, Ireland might be near the middle of the table at the moment. Google however deserve a yellow card for the privacy-invasive way in which they seem to have implemented their part of the overall tracing system."

More information: Leith et al., Contact Tracing App Privacy: What Data Is Shared by Europe's GAEN Contact Tracing Apps. (2020). www.scss.tcd.ie/Doug.Leith/pub … cing_app_traffic.pdf

Provided by Trinity College Dublin