Contact tracing apps: Google can spy on users even better

Posted by Press Office | September 24, 2020 | Current news, data protection, press releases, slider

From a data protection perspective, European contact tracing apps can be given a positive verdict. This is the verdict of a study carried out on behalf of the national health authorities. The German solution actually performs best from a technical point of view in terms of data protection. And yet the use of contact tracing apps is problematic from a data protection perspective, which is less due to the apps themselves than to Google Play Services, in which the Google/Apple Exposure Notification (GAEN) framework for contact tracing of state corona warnings apps has been integrated.

As is well known, two components are required for contact tracing to work with the Corona-Warn-App: the contact tracing app itself and the interface (API) on the Android or Apple smartphone. Only an interaction of both components enables the exchange of contact IDs or the necessary Bluetooth information of the smartphones. While the app was implemented in a data protection-friendly manner in most European countries, the Google interface in particular, due to the connection to the Play Services, is to be classified as particularly problematic in terms of privacy protection, according to the researchers.

Android smartphones connect to Google servers about every twenty minutes and transmit a lot of personal data such as telephone number, email address or IP address. Just by regularly recording the IP address, Google is able to track where a user is.

The data flows are already created by the pre-installed Google Play Services and even occur when other Google Services and settings are deactivated. This means: Basically, every Android user is affected by the unprovoked data transmission to Google - even without using contact tracing apps that are based on the GAEN framework.

In order for contact tracing apps to work and exchange Bluetooth signals with other smartphones, permanent access to the “location determination” or location function must be guaranteed. Android smartphones use GPS, mobile or WiFi networks and also Bluetooth radio to determine their location - it is not possible to deactivate individual components. That means: If you want to use the Corona-Warn-App, you have to activate the whole bundle of location signals and thus provide Google with your exact whereabouts permanently.

Now you could say: "This is all known, this is part of Google's industry practice and has nothing to do with the Corona App". However, the explosive nature of such a data usage practice is heightened by the use of the Corona-Warn-App. The data collection mania of corporations in combination with an app that citizens are encouraged to use by their government for the purpose of health protection, but which sends all the more data to the corporation is unacceptable. A Corona warning app is intended to ensure healthy, not transparent citizens. This once again makes the problematic business practices of the so-called data octopuses clear. Here the legislature has a duty to remedy the situation.

Further information on the topic:

"100 days of Corona-Warn-App: Government warns for increased use" on https://www.tagesschau.de/inland/corona-warn-app-133.html from September 23, 2020.
Summary of Trinity College Dublin study “Contact Tracing App Privacy: What Data Is Shared By Europe’s GAEN Contact Tracing Apps”.

If you have any questions, you can reach us on the telephone number 0711/615541-23.
Further information on freedom of information can be found on the Internet at www.baden-wuerttemberg.datenschutz.de or at www.datenschutz.de.
www.beteiligungsportal-bw.de
The press release is available here as a PDF.

Share:

```
.post-footer .rating-stars #rated-stars img.star-on,
.post-footer .rating-stars #rating-stars img.star-on {
background-color: #868682;
}
```