NORTON ROSE FULBRIGHT

Contact tracing apps in Germany

A new world for data privacy

As of June 23, 2020

The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. To aid the safe lifting of current public health restrictions, new technologies are being developed – contact tracing apps – and rolled out to automate labour intensive tasks critical to containing the spread of the virus. Our contact tracing survey summarises the principal regulatory and policy issues applicable to contact tracing across a range of key jurisdictions in real time.

Is technology being used by the government to monitor and control the spread of COVID-19 (e.g. contact tracing app, CCTV, cell phone location data, credit-card history)?

The German Federal Government has launched an official App "Corona-Warn-App" on June 16, 2020 which was developed by SAP and Telekom on behalf of the German Federal Government. The "Corona-Warn-App" is based on the Privacy-Preserving Contact Tracing ("PEPP-IT"). The Corona-Warn-App and backend infrastructure will be entirely open source - licensed under the Apache 2.0 license. The Corona-Warn-App is being developed on basis of the Exposure Notification Framework ("ENF") provided by Apple and Google, which will uses Bluetooth Low Energy technology ("BLE"). The Corona-Warn-App will collect pseudonymous data from nearby mobile phones using BLE. As soon as two users approach each other within a distance of about two meters and remain at this distance for fifteen minutes or longer, their apps will exchange data via BLE. If an user tests positive for COVID-19, the user can feed the test result into his/her Corona-Warn-App. The Corona-Warn-App will then anonymously inform all stored contacts. The data will be stored locally on each device preventing access and control over data by authorities or a third party.

Currently there is one other app available in Germany launched by Robert Koch Institute (German federal government agency and research institute responsible for disease control and prevention, "RKI") – "Datenspende-App". This app does not yet trace contacts, but only general movement and fitness information. The app collects the user data using their fitness tracker and sends it to the RKI. The RKI analysis anomalies in the data, which is sorted by postcode: As pulse rate, sleep rhythm and activity level change due to an acute respiratory disease, the RKI claims that it can also indicate a Covid-19 disease having this data.

What are considered to be the major privacy concerns in relation to the app in your jurisdiction (in relation to its use (a) by the government; and (b) by private sector organisations)?

"Corona-Warn-App": - There are no major privacy concerns as the Corona-Warn-App has been designed with a special focus on privacy from the beginning. The German Data Protection Authorities generally support the Corona-Warn-App and only expressed minor concerns, but less on the Corona-Warn-App itself but rather on the way it may be used:

- As Apple and Google, as providers of the operating systems, have access to all data that runs over their interfaces, there are some concerns regarding the Intension of Apple and Google.
- The voluntary aspect of the Corona-Warn-App could be undermined through social or economic pressure which could be specifically enforced by employers. It is proposed that a special accompanying law (which has not been passed, drafts of opposition parties available) is required to address these issues.

The Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) announced that the use of the telephone-Tan-registration is not an optimal solution because the complete anonymity of the user will no longer be guaranteed.

"Datenspende-App": There are several concerns indicated by Chaos Computer Club, a cyber security NGO, in particular:

- RKI can directly retrieve the fitness data from the provider of the fitness tracker or Google Fit and only then the data will be pseudonymized (except Apple Health). As the RKI also stores access data to the fitness tracker, it can be used to access complete history and names of the users.
- Easy reversal of the pseudonymisation and the insecure handling of the confidential pseudonym as the app does not use a standard browser but an embedded web view which is insecure due to man-in-the-middle attacks.
- The RKI server exposes additional functionality such as a management and admin interface as well as a SOAP API via the Internet. This increases its vulnerability.

App details

1. What is the name of app

"Corona-Warn-App" and "Datenspende-App"

2. Is the app voluntary?

Yes

3. Is there any suggestion that use of the app and a clean result may be necessary to enter workplaces or any commercial or public buildings (or is this explicitly or implicitly prohibited)?

No

The German Federal Government states that the use of the Corona-Warn-App is voluntary which implies that there are no negative consequences in connection with the refusal to use the Corona-Warn-App in workplace or public/ commercial buildings.

German data protection conference declares that access to public institutions, workplaces, sport facilities and restaurants cannot be made conditional on the use of the Corona-Warn-App.

Individuals who have been notified by Corona Warn App of the infection risk can then self-isolate to help stop the spread of the virus.

4. What information is required to register for the app? Is the information collected considered excessive?

Corona-Warn-App: No

Registration for the Corona-Warn-App does not require personal data.

Datenspende-App: Yes

Post code, age, gender, weight, height and data collected by fitness trackers.

5. Is GPS or Bluetooth used?

Bluetooth

6. Is data stored on a centralised server?

Corona-Warn-App: No

The data is only stored on the user's devices.

Centralized server is only used to storage the pseudonymized lists of contact-IDs.

Datenspende-App: Yes

The fitness data is stored on the server of the fitness tracker provider and analyzed on RKI's server.

7. Does the identity of the infected user get captured centrally?

No

8. Is the identity of the infected user disclosed to proximate users or public health authorities? Is it disclosed to anyone else?

No

9. Is consent needed to share data with other users/ upload the data to a centralised system?

No

Results of positive tested persons by a health authority will only be shared if the tested person wishes to inform the Corona-Warn-App of his updated status. To prevent abuse, the person has to verify his test results through QR-Code or via telephone-TAN-registration. The smartphones of persons who have had contact to the positive tested person will be automatically informed but without disclosing the identity of the person infected.

10. Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?

No

No, the app is designed to assist the authorities with finding the infection routes so that those who have been infected can self-isolate.

11. Does the app incorporate "privacy by design" and was a privacy risk assessment completed?

Corona-Warn-App: Yes

All data is psedonymized. Each smartphone will act as a beacon that constantly sends out its own temporary ID while searching for IDs from other smartphones. To ensure complete privacy and prevent tracking of user movement patterns, the IDs sent will be temporary and change every 15 minutes. New IDs are derived from a key that changes daily through a cryptographic process. The collected IDs of other users will be stored locally on each individual smartphone within the ENF. If users have tested positive for COVID-19, they can provide the app with a verification of their positive test by selecting the option to share their own pseudonymized IDs. Their temporary keys from the last 14 days will be uploaded to a server. At regular intervals, the app pulls from the server a list of pseudo IDs of users who have voluntarily reported that they are infected.

The app compares their pseudo IDs with those stored on the smartphone to determine whether there has been any exposure. If a user has been exposed to other infected users , he or she will receive a notification and recommendations on what to do. This information will only be stored on the user's smartphone and will not be provided to a third party. The app provider or a third party is unable to determine with whom an individual has had contact. No tracking information, behavioral profiles or similar patterns will be processed centrally.

Datenspende-App: Generally yes

The user's smartphone will only send psedonymized data to the RKI. However, due to a recent report published by Chaos Computer Club, there are concerns about whether the app incorporates "privacy by design".

12. How long will the data be kept for, are there clear lines around timing?

Yes

The temporary keys of pseudonymized IDs among users who have tested positive will be uploaded to a server for 14 days.

13. Has data security been addressed expressly (e.g. encryption)?

Yes

The Federal Commissioner for Data Protection and Freedom of Information stated that the level of data security is sufficient. He explained that there are vulnerabilities but there is no reason why the Corona-Warn-App should not be downloaded.

14. Are there clear limitations regarding who may have access to the data?

Datenspende-App: Yes

Access is emailed to the RKI.

Corona-Warn-App: Unknown

It is still unknown how the infection routes will be determined by the competent infection protection authority and RKI. They will probably have access to aggregated data only. According to the available information, only those individuals who may have been infected will be informed of the infection risk.

15. Are there clear limitations on the purposes for which the government may use the data?

Yes

Assisting the authority to find out the infection route.

16. Is the government of your country bound by privacy laws in respect of the contact tracing data?

Yes

17. Has the regulator commented/ provided guidance on the technology?

Yes

The state data protection commissioner of Baden-Württemberg has defined the general requirements for an official app:

- The terms of use for the app must be transparent and clear.
- The app may be only advertised as having a supporting but not a 'blessing' function.
- It is recommendable to enact a legal basis for the use of the app which clearly stipulates the legal framework.
- Neither the use nor the non-use of the app may be subject to the user's advantage or disadvantage. Even if there are not enough users for the app, the voluntary nature of its use must never be turned into an obligation.
- The app's source code must be disclosed as it provides information about the processing mechanisms and data transfers the app actually provides for.
- Any governmental access to the data - whether by researchers looking for ways out of the health crisis, by the police, who are responsible for ensuring compliance with quarantine orders, or by the public prosecutor's office, for whom access to the app data could yield significant insights into ongoing criminal proceedings - must be definitely ruled out.
- Any secondary use of the data – for example for science and research – must be clearly ruled out. This does not exclude the possibility that users of the app may also release their data for other purposes. However, "releases" should not take place in the tracing app itself, but in separate, independent procedures.
- All data collected should be deleted without delay according to clearly defined criteria - and should not be kept longer than necessary to protect against the diffuse risk of a possible second wave.

18. Are there any private sector initiatives you are aware of to use/ integrate the app or the information from the app (e.g. to reflect the results back to workforces)?

No

Contacts

Christoph Ritzer
Partner
Frankfurt
Tel +49 69 505096 241
christoph.ritzer@nortonrosefulbright.com

Chris Cwalina
Global Co-Head of Data Protection, Privacy and Cybersecurity
Washington DC
Tel +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Marcus Evans
Head of Data Protection, Privacy and Cybersecurity, Europe
London
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Ffion Flockhart
Global Co-Head of Data Protection, Privacy and Cybersecurity
London
Tel +44 20 7444 2545
ffion.flockhart@nortonrosefulbright.com

Anna Gamvros
Head of Data Protection, Privacy and Cybersecurity, Asia
Hong Kong SAR
Tel +852 3405 2428
anna.gamvros@nortonrosefulbright.com