Contact tracing apps in Germany
A new world for data privacy

As of May 26, 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 plans to launch by mid-June an official app “Corona-Warn-App” which is currently being 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”) technology. The app and backend infrastructure will be entirely based on open source code - licensed under Apache 2.0. The app is being developed with the Exposure Notification Framework (“ENF”) provided by Apple and Google, which will use Bluetooth Low Energy technology (“BLE”). The app will collect pseudonymous data from nearby smartphones using BLE. The data will be stored locally on each device, thus preventing any access or control over the data being available to authorities or other third parties.

Currently there is an app available in Germany launched by Robert Koch Institute (German federal government agency and research institute responsible for disease control and prevention, “RKI”) called “Datenspende-App”. This app traces general movement and fitness information using the fitness tracker only but not contacts and then sends the data to the RKI. The RKI will analyze anomalies in the data. It claims that the app can help detect COVID-19 by analyzing changes in the user’s pulse rate, sleep rhythm and activity level.

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”: As providers of the operating systems, Apple and Google will have access to all user data. There are some concerns regarding their plans to develop the app.

“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). RKI may have access to the activity history and the names of the users.
- Easy reversal of the pseudonymisation and insecure handling of the confidential pseudonym: the app does not use a standard browser but an embedded web view which is insecure due to possible 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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>What is the name of app</strong>&lt;br&gt;“Corona-Warn-App” and “Datenspende-App”</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Is the app voluntary?</strong>&lt;br&gt;Yes</td>
</tr>
<tr>
<td>3.</td>
<td><strong>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)?</strong>&lt;br&gt;No&lt;br&gt;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.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>What information is required to register for the app? Is the information collected considered excessive?</strong>&lt;br&gt;Corona-Warn-App: No&lt;br&gt;Registration for the app does not require personal data.&lt;br&gt;Datenspende-App: Yes&lt;br&gt;Post code, age, gender, weight, height and data collected by fitness trackers.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Is GPS or Bluetooth used?</strong>&lt;br&gt;Bluetooth</td>
</tr>
<tr>
<td>6.</td>
<td><strong>Is data stored on a centralised server?</strong>&lt;br&gt;Corona-Warn-App: No&lt;br&gt;At the users’ devices.&lt;br&gt;Datenspende-App: Yes&lt;br&gt;The fitness data is stored on the server of the fitness tracker provider and analyzed on RKI’s server.</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Does the identity of the infected user get captured centrally?</strong>&lt;br&gt;No</td>
</tr>
<tr>
<td>8.</td>
<td><strong>Is the identity of the infected user disclosed to proximate users or public health authorities? Is it disclosed to anyone else?</strong>&lt;br&gt;No</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Is consent needed to share data with other users/ upload the data to a centralised system?</strong>&lt;br&gt;No</td>
</tr>
<tr>
<td>10.</td>
<td><strong>Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?</strong>&lt;br&gt;No&lt;br&gt;No, the app is designed to assist the authorities with finding the infection routes so that those who have been infected can self-isolate.</td>
</tr>
<tr>
<td>11.</td>
<td><strong>Does the app incorporate “privacy by design” and was a privacy risk assessment completed?</strong>&lt;br&gt;Corona-Warn-App: Yes&lt;br&gt;All data is pseudonymized. 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.</td>
</tr>
<tr>
<td>Datenspende-App: Generally yes&lt;br&gt;The user’s smartphone will only send pseudonymized 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”.</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td><strong>How long will the data be kept for, are there clear lines around timing?</strong>&lt;br&gt;Yes&lt;br&gt;The temporary keys of pseudonymized IDs among users who have tested positive will be uploaded to a server for 14 days.</td>
</tr>
</tbody>
</table>
13. Has data security been addressed expressly (e.g. encryption)?
Yes

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

© Norton Rose Fulbright LLP. Extracts may be copied provided their source is acknowledged.
EMEA 24297 - 05/20