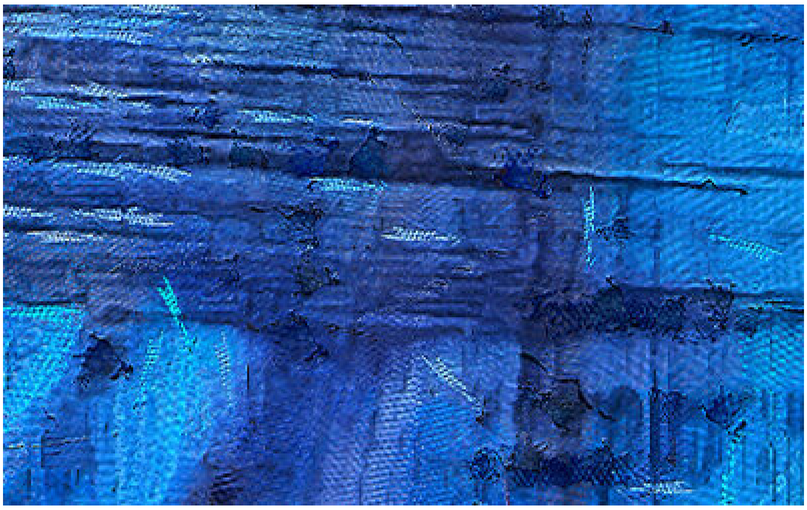
MAYER | BROWN



CYBERSECURITY | COVID-19 Tracing App Released in Germany

On 16 June 2020, the "Corona-Warn-App" ("the App") was released by the Federal German government. The tracing App, which uses Bluetooth technology, records which smartphones have come close to each other. If a user has tested positive and has shared this in the App, it will subsequently notify other users that they have been near an infected person. Notified users can then voluntarily be tested, even without symptoms, at the cost of the public health system. Seven days after its release, the App has already been downloaded by 12.2 million people in Germany.

This is the second App released by the government to help fight the pandemic. The first one, called "Corona Data Donation App", was released in early April and aims at estimating potential COVID-19 infections by analyzing health data from users, collected by a fitness watch and made available to the Robert Koch Institute (a Federal Institute on behalf of the Federal Ministry of Health) through the app[1]. The two apps are thus complementary, though the second one seems to be much more successful. This first app had about 500,000 users a month after its release.

How Does The COVID-19 Tracing App Work?

App users' smartphones continuously generate random IDs—a sequence of random digits that change every 10-20 minutes and are created in encrypted form from randomly generated keys that change every 24 hours. The random IDs are exchanged with other App users via Bluetooth LE (Low Energy). If the encounter exceeds 5 minutes, the smartphones store each other's IDs along with information on the date and duration of the contact and the Bluetooth signal strength (together called the "associated metadata"). This data is stored on the smartphone for 14 days.

If a user is infected with COVID-19, he or she has the option of uploading the test result onto the App. The App retrieves from the App's server systems several times a day a list with random IDs of users who have tested positive for COVID-19. Each App user's smartphone compares this list to the list of random IDs to which it has been in contact and stored in its operating system in the last 14 days. If there is a match, the App analyzes the associated metadata using an algorithm to determine the risk of infection for this precise App user, taking into account, for instance, the distance between the smartphones, estimated on the basis of the Bluetooth signal strength, and the duration of contact. The App then informs the user that he or she has been in contact with a person infected with COVID-19 and gives recommendations as to next steps. The App only provides the algorithms. The analysis of the data and of the risk of infection is performed locally by the operating system of the smartphone. No one, not even the Robert Koch Institute, Google, Apple or any third parties, receives the information that the user has been in contact with someone infected with COVID-19 and the result of the infection risk analysis.

Sharing Information On Tests And Test Results Through The App Or A Telephone Hotline

After taking a COVID-19 test, App users may scan a QR-Code provided by the test laboratory. If the lab is connected to the App system, the user is notified through the App when test results are available. Several organizational and technical measures have been implemented to secure the transmission and storage of information.

If a user has tested positive for COVID-19, the user may call a hotline that has been set up in connection with the App. The purpose of the call is to verify the diagnosis to avoid false disease allegations that create incorrect warnings and risk values. Users are asked a few questions to check the plausibility of the call, and need to share their telephone number. The hotline staff will obtain a TAN on behalf of the user and call him or her to communicate it, so that the user can indicate it on the App to communicate the positive test result. The user’s telephone number is deleted after an hour at the latest.

Data Processing and Legal Basis

The legal basis of the processing of personal data in relation to the App is the data subjects’ consent pursuant to Art. 6(1)(a) and Art. 9(2)(a) GDPR.

Data regarding App users’ name, address and location are in no way processed. The App servers are located in Germany or Europe, and only two companies (T-Systems International GmbH and SAP Deutschland SE & Co. KG) are charged with the operation and maintenance of parts of the technical structure of the App, thus acting as data processors. Data is not processed by any other parties.

Plus and Minus

Currently, the App is only available on the newest models of Android and iPhone smartphones. On the latter, the operating system iOS 13.5 must be installed, which is not available for devices older than the iPhone 6s or the iPhone SE. Also, the App is currently not available for smartphone users who do not have a German App-Store account, for instance if the smartphone account is based abroad. The German government has announced that it is in exchange with Apple and Google to see if it is possible to make the App available in earlier smartphone versions as well as in stores in other countries.

Some criticism has been expressed by the Federal Commissioner for Data Protection and Freedom of

Information ("*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*", "BfDI"), Professor Ulrich Kelber. He accompanied the project and recommended that the data protection impact assessment be published before release of the App to increase the public's trust. This was not done. Also, he criticized the additional use of a telephone hotline, as this solution "*cannot keep up with a completely pseudonymous use of the App via the automated procedure*". In his view, the Robert Koch Institute and the Ministry of Health must create the necessary conditions as quickly as possible so that the automated procedure can be used by as many App users as possible. Furthermore, in line with the Guidelines of the European Data Protection Board ("EDPB"), he warns that third parties shall not be granted any access to data, for instance as a condition to accessing public transport or shops. In spite of these criticisms, he approves of the App from a data protection perspective.

Compliance with the EDPB Guidelines

It is worth noting that all of the recommendations of the EDPB[2] have been followed, in particular:

- Respect of the principles of (i) privacy by design (the App was developed by the government and the Robert Koch Institute by embedding privacy considerations), (ii) data minimization (indeed no more personal data is processed than necessary), (iii) purpose limitation (personal data is only processed for the purposes for which the data has been collected), and (iv) storage limitation (data deletion is automatic once data is no longer needed for the purposes it was collected);
- No location data is processed;
- Data is processed largely on the smartphones of the users, and not stored at a central server[3];
- Technical and organizational measures have been taken to reduce substantially the risk of re-identification of App users and to safeguard the cybersecurity of the App;
- The controller is the Robert Koch Institute and the source code of the App has been published which helps build users' trust (even if it may increase cybersecurity risks, as was the case with the Dutch app[4]).

Conclusion

The App is widely perceived as a sophisticated technical solution relying on a carefully designed Data Protection and Cybersecurity system assuring a high level of data protection. Its success will depend on how many people use the App which is at this time unpredictable. It has certainly gotten off to a good start.

Authors

- Ana Hadnes Bruder, Master en Droit, LLM
- Dr. Ulrich Worm

Related People

- Mark A. Prinsley
- Oliver Yaros
- Charles-Albert Helleputte
- Diletta De Cicco
- Régine Goury

[1] https://www.covid19.law/2020/04/covid-19-app-released-in-germany/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

[2] For more information please access our Legal Update: https://www.mayerbrown.com/en/perspectives-events/publications/2020/04/eu-positions-on-contact-tracing-applications-during-covid19–no-lockdown-for-privacy-cybersecurity.

[3] Differently than the solution adopted in the UK: https://www.mayerbrown.com/en/perspectives-events/publications/2020/05/nhs-launches-contact-tracing-app-to-combat-covid19.

[4] More information under "Risks Identified: 'Grave Intrusion' into Privacy" in our Legal Update: https://www.mayerbrown.com/en/perspectives-events/publications/2020/04/eu-positions-on-contact-tracing-applications-during-covid19–no-lockdown-for-privacy-cybersecurity.