The "voluntary" corona app

For a gradual withdrawal of the corona contact restrictions, the German government is counting on a broad acceptance of this app, which enables reconstruction of an infected person's contacts, and which can be downloaded after Easter. The (justified) fear of the virus is used to "voluntarily" administer an authoritarian, highly effective tool to a large part of the population. In this article we criticize not only the technical construction of the app, but also its social-technocratic consequences. Even if the logging of contacts were done completely pseudonymously, we would have to urgently warn against this app. At the moment when (even anonymous) behavioral data is collected across the board, the predictive models that are trained with it are capable of classifying entire populations into risk groups and managing them algorithmically. In addition, a simple software update turns the app into an effective tool for restricting individuals. Hence our clear rejection of the Corona App!

An international team consisting of around 130 scientists, IT developers, data protection officers and soldiers is currently working on a project called Pan European Privacy-Protecting Proximity Tracing (PEPP-PT) to develop software to restrict the spread of the SARS-CoV-2 virus. The Robert Koch Institute (RKI), the Heinrich Hertz Institute (HHI) and the Federal Office for Information Security (BSI) are among the German partners involved. The Federal Data Protection Commissioner is also accompanying the development and Bundeswehr soldiers are among those testing the app. With the exception of RKI, they are not listed on the project's website. The HHI is subsumed under Fraunhofer. So far, researchers and institutes from eight countries are involved in the development: Austria, Belgium, Denmark, France, Germany, Italy, Spain and Switzerland.

To contain the spread of the infection, people who have come into contact with infected persons should be warned as early as possible. If people show symptoms, they are already contagious. Therefore, after a positive diagnosis, all mobile phone owners whose devices were in the vicinity of the infected person should be notified. If there are many individual approaches and software solutions, each of which is used by only a small part of the population, this concept will not work. For this reason, the intention is to create a common basis that reaches a critical mass as quickly as possible. We are talking about a common platform: a client/server reference implementation, but also a software framework on which smartphone apps can be built. These smartphone apps, which users install on their phones, form an essential part of the system. In Germany, RKI and HHI are working on such an application. In order to interrupt chains of infection effectively, the researchers are aiming for a user base of about 60 percent of the population. In Germany this would be 50 million people. So far, there is no app in Germany that is not pre-installed on smartphones and has to be deliberately downloaded, which has so many users. However, even a smaller proportion could help to at least slow down the spread. According to Bitkom, 81 percent of all people in Germany over the age of 14 own a smartphone. Normal mobile phones and older devices do not yet support the necessary Bluetooth standard. In particular, not all seniors, for whom the virus is particularly dangerous, can be warned. Therefore, the researchers are considering distributing Bluetooth bracelets or other wearables in the future. According to a representative survey (as of 31.03.2020), more than 70 percent of those questioned would definitely or probably use such an app. The majority say they would comply with the app's requests and quarantine themselves if they came into contact with an infected person. According to surveys, a large part of the population in Germany would be prepared to give up part of their privacy in order to stop the virus. The PEPP-PT platform

is scheduled for completion on April 7. RKI and HHI want to release the app for German users about a week later.

The system is intended to be understood as an alternative to the repressive and invasive approaches of other countries. Instead of collecting masses of sensitive location data, monitoring users or putting infected persons in a digital corona pillory, PEPP-PT should be completely voluntary and protect users' data. The operators promise to protect the privacy of users of the software. The identity of the users remains protected at all times. Neither doctors nor the operators of the platform can identify individuals. Good PR is provided by newspapers write about anonymisation of users, although it is pseudonymisation. The PEPP-PT model also does not seem to require 100 percent privacy-by-design. However, according to the website, which has very poor information on the app so far, the specifications and source code are currently only available for members of the consortium. We say: disclose code and all documents, otherwise we don't believe anything. And not just any client reference implementation, but the whole specification and all server code.

Critique 1: Technical details

The following technical details are based on the little information available on the PEPP-PT website and reports from Netzpolitik.org. The apps assign each device a temporarily valid, authenticated and randomly generated identification number (ID). The temporary, randomly generated ID functions as a pseudonym, which is intended to reliably protect the individual's identity. It is changed at regular intervals (we are talking about 30 minutes) and is not supposed to be associated with the phone. Furthermore, nobody should be able to identify the individual associated with a particular pseudonym. Every PEPP-PT phone (meaning a smartphone on which the app is installed) sends its current ID over a short distance using Bluetooth radio technology (Bluetooth low-energy) and at the same time scans the environment and records which other smartphones which have PEPP-PT software installed are within range. When two devices approach each other, the apps store the temporary ID of the other smartphone. The approach of phones of other PEPP-PT users is recognised by measuring radio signals (Bluetooth etc.). The data initially remains encrypted on the smartphone, allegedly inaccessible by anyone. Due to the limited information available, it is unclear as to how this was implemented cryptographically. Not every instance of two PEPP-PT phones coming within range of one another is stored. Only if PEPP-PT phone A is in the vicinity of PEPP-PT phone B for an epidemiologically sufficient period of time (we are talking about 15 minutes at a distance of 1.5 meters), then the current temporary ID of phone B is stored in the encrypted proximity history of A (and vice versa) in the encrypted proximity history stored locally on the phone. It remains to be seen whether the 15-minute interval is a reasonable length of time, because coughing on the bus or in the shop only takes a few seconds, and short calls can last 1-2 minutes. That is enough time for the infection to be transmitted. It is also u
nclear as to what is actually stored. According to the PEPP-PT website, no geolocation, no personal information, unique device identifiers such as the IMEI number of the smartphone or other data that would allow the user to be identified are logged. It further states that the pseudonymous approach history cannot be viewed by anyone, including the user of phone A. Older events in the approach history are deleted when they become epidemiologically insignificant. "We only measure how long and how close two people have come across each other," says Thomas Wiegand, who heads the HHI. The virus does not care where the meeting took place. "This is the only information of epidemiological significance." After 21 days, the data is automatically deleted. Instead of tracking, PEPP-PT relies on tracing - it is not intended to track people's movements, only their contacts. On the smartphone, a list of IDs with time stamps is created, behind which the people who you may have infected are hidden, or who may have transmitted the infection to you.

To reduce false alarms, researchers have examined all widely used smartphone models and measured their signal strengths, since they may differ in some cases. Bundeswehr soldiers helped calibrate the technology to detect, for example, whether there was a glass pane or other obstacle between two contacts that prevents transmission of the virus. The accuracy and reliability of the claim that someone was within a 1.5 meter radius of another person using Bluetooth is extremely doubtful.

Use of Proximity History

In the event that a user has not been tested or tests negative, the approach history remains encrypted on the user's phone and cannot be viewed or transmitted by anyone. However, if the user is confirmed to be SARS-CoV-2 positive on phone A (i.e. usually already ill with Covid-19), then this person transfers the current list of IDs that is locally stored in their proximity history to a national central server. That is not straightforward. Doctors, laboratories and health authorities must confirm the report. It is therefore imperative that a positive diagnosis be made. The health authorities then contact user A and provide her with a TAN, which ensures that potential malware cannot infiltrate the PEPP-PT system with false infection information. The interface should be encrypted and secret so that the identity of the infected person remains protected. The user uses this TAN to voluntarily transmit information to the server of the national service provider, in Germany for example at the Robert Koch Institute, which enables notification of PEPP-PT apps of people who have come into contact with the infected person, and who are therefore potentially infected. Currently, this will only be done voluntarily. The central server will only find out what other temporary IDs this smartphone has been in contact with if the user agrees. Social pressure is concealed.

What happens with the data on the server?

The consortium writes that since the proximity history contains pseudonymous identifiers, the server cannot use these IDs to determine which people are behind them, but it can notify all affected contacts via the app and ask them to get tested. This is because no personal data is required to display a message on the smartphone. All that is required is a push token, a unique app device identifier, to send a push message to the device via Apple's or Google's push notification gateways. This push token is generated when the app is installed on the phone. At the same time, the app stores both the push token and the temporary IDs it sends on a central server.

In this way, the smartphones can be addressed solely on the basis of temporary IDs and push tokens, without it being possible to determine the identity of the persons carrying these smartphones. For this purpose, however, it is necessary that push tokens and all current temporary IDs generated for each account, including a time stamp showing when they were generated, are stored on the server. The server must be trusted to delete epidemiologically irrelevant data after 21 days - and not to continue storing it for big-data purposes. As soon as the push token is linked to data from the provider (push token assignment to device ID, IMEI, or phone number), the user becomes easily identifiable.

Criticism 2: Although anonymous, we're still training AI

The PEPP-PT app is not intended to access personal data of the individual. But dangers do not only arise directly from the digital exposure of individuals, but also from the fact that the resulting data collection enables algorithmic procedures for population control. Pseudonymised mass data serve to train artificial intelligence (AI), e.g. in the context of predictive analyses. At the moment that behavioral data is collected almost everywhere and (even if it is anonymous), the predictive models trained with it are able to divide whole populations into risk groups and manage them algorithmically. Data-based algorithms can then divide society into invisible social classes, for example, with regard to who, on the basis of their movement patterns, supposedly poses a particular health or safety risk, because the movement profile indicates that someone has spread the virus in a particular way or who deserves priority access to scarce medical resources such as respiratory care. Algorithmic scoring and decision-making procedures are based on an anonymous comparison with the data of many other individuals. Therefore, people can potentially harm other individuals and groups by passing on their own (even anonymised or pseudonymised) data and, conversely, be potentially affected themselves by the data passed on by others. This danger is ignored in the brief debate about the PEPP-PT App and even when anonymous telecom data or anonymized Google position data is passed on. It is also not the subject of effective data protection efforts. For example, the basic data protection regulation DSGVO does not protect against the use of anonymised data for predictive algorithmic decisions, risk classification (scoring) and behaviour-based unequal treatment of individuals or groups. In this sense, everyone who uses the PEPP-PT App has to be aware of this danger. For example, the basic data protection regulation DSGVO does not protect against the use of anonymised data for predictive algorithmic decisions, risk classification (scoring) and behaviour-based unequal treatment of individuals or groups.

In this sense, everyone who uses the PEPP-PT App contributes to such unequal treatment, where the distinction between anonymous and personal data is outdated because it is irrelevant!

Criticism 3: "Voluntariness"

"Please understand that for your own safety and the safety of our employees we can only transport demonstrably non-infected persons". This could be the explanation of the Deutsche Bahn at all vending machines and ticket counters, which offers its service "until the end of the corona crisis" only to passengers with a modified PEPP-PT app. The PEPP-PT-App 2.0 would report all contact events directly to the server "on request" (again absolutely voluntarily and only with the consent of the users) - quasi with a free TAN. Furthermore, no personal data, including location data, would be recorded. Only if the real-time evaluation of all contact events of the last 14 days shows no connection to an infected person, or to a person who has previously had contact with an infected person, the QR code of the electronic train ticket would give a gree light, i.e. "probably not infected". According to the same principle, shopping malls, concert halls, stadiums, ... could make access or payment at the ticket office conditional on showing "green" status on a PEPP-PT app. This would be a massive restriction of freedom of movement - if you want to be "free", you have to submit to the app (and the server infrastructure behind it). The "voluntary" PEPP-PT app becomes a tool for distinguishing between individual social participation and the "voluntary" PEPP-PT app. If you want to take the train, you would need this PEPP-PT-App 2.0. The state does not "prescribe"

this extended PEPP-PT-App, it only makes it available. Economic actors - in our example Deutsche Bahn - would only offer their services to those who agree to this advanced version of the PEPP-PT-App. Government and service providers would act in the spirit of an overarching responsibility for the common good. Who wants to complain ...? Many of the social-scoring models currently being tested in China are based on this form of "voluntary action". Anyone who does not participate or does not fulfil the required characteristic (according) can be "voluntarily" excluded from public life without a prohibition order: The PEPP-PT App may pave the way for the use of individual inclusion / exclusion mechanisms of future social point systems in Germany. A final point is that data is supposedly to be kept confidential may be used for criminal prosecutions once this use has been approved. Where there is a trough, pigs come. There are many examples (such as the registration of the electronic toll). In addition, there may be an official order to stop the deletion of collected data. Currently, persons must actively release the data in their proximity history. But with a software update it is easy to change that, so that all contacts are always uploaded. This creates a huge amount of data that can be used for big data purposes. If all contact IDs are always transmitted (i.e. no longer only voluntarily when a person is infected), the server can also create traces and establish connections who meets whom and how often. In cooperation with telecommunications providers to resolve IP addresses, law enforcement agencies could then resolve who is hiding behind the IDs.

capulcu, 5. April 2020
capulcu.blackblogs.org