Fraunhofer

PROXIMITY TRACING IN THE CONTEXT OF CORONA:

FRAUNHOFER'S APPROACH FOR GERMANY

THE SITUATION AND TECHNICAL IMPLEMENTATION

Summary:

Proximity tracing apps are a digital option for efforts to contain the coronavirus pandemic currently underway. Various assumptions and prejudices figure prominently in the debate on the use of proximity tracing apps in Germany and Europe. The Fraunhofer-Gesellschaft has **developed an approach of its own for a German proximity tracing app**. Using **Bluetooth technology on cell phones to measure distance and time**, it is to enable digital messaging to notify individuals who are at **risk of a SARS-CoV-2 infection**. Germany already has functioning and established pandemic control practices and procedures in place.

The aim of this project is to develop an IT system with **digital tools to augment health authorities' practices and to help implement the corresponding recommendations of the Robert Koch Institute (RKI)**. This is to be done by way of a digital process that measures distance and time using Bluetooth technology on cell phones and notifies people who are at risk of a SARS-CoV-2 infection. The **overall system's functionality derives from the legal mandate of public health authorities** and has to meet a number of specifications for it to be used. This project addresses these demands directly.

Work on the German app commenced in early March 2020 at the **participants' expense**, **with the support of base funding from the Federal Ministry of Education and Research** (BMBF), and with a feasibility study funded by the Federal Ministry of Health (BMG). From the outset, this project was geared to create a **pan-European solution that complies with data privacy laws**. **French partners** are on board to help develop the system. This **cooperation** was stepped up in recent weeks to achieve full compatibility.

The project's entire approach is underpinned by the conviction that the **public healthcare system must retain sovereignty** over the criteria for **conducting risk assessments, recommending actions** and **sharing feedback** within this type of system. The proposed system **does not collect or process data** such as information about the place, phone numbers, names, and the like when the app is used. The use of the system via an installable app will be **voluntary**. Users may **uninstall** the app at any time without the service on the server being able to identify who deactivated the app. Registration **does not require personal data** such as the individual's name or phone number. The intention is to maximize support for the app on available devices by **collaborating with the operating system vendors Google and Apple**. The system's design factors in the principle of **data minimization** in keeping with **data protection regulations**.

1. The situation in Germany

The COVID-19 pandemic prompted the German Bundestag to declare an epidemic situation of national significance on March 16 and 23, 2020. Contact restrictions and closures were then imposed nationwide. The states issued shelter-in-place orders to contain the exponential spread of the disease.

1.1 The legal situation and duties of health authorities and testing labs

As it stands at the time of writing, public health authorities have the lead role in containing the outbreak by disrupting the chain of infections. The German Protection Against Infection Act (IfSG) requires laboratories and attending physicians to notify their designated public health department when individuals test positive for or are diagnosed with SARS-CoV-2. The standard practice is for a representative of the public health department to then contact these individuals or their attending physicians and/or relatives. During this interview, the representative asks the infected individual about contacts of epidemiological relevance during the suspected contagious phase; that is, the incubation period two days before the onset of symptoms. This yields a contact list for tracing and follow-up. The public health department assesses on a case-by-case basis if and which actions are to be taken. Actions taken for individuals who have been in close contact can include quarantine and active health monitoring. An individual may be isolated if there is reason to believe he or she has been infected. The **RKI's recommendations** on questions such as when to quarantine serve as a guideline.

This practice has proven its merits. It is essential to disrupting the chain of infections. The sooner the authorities identify contact persons and the earlier they are quarantined or isolated, the more successful their efforts to disrupt the chain of infections will be. This process needs to be accelerated and improved.

1.2 The current state of epidemiological knowledge

Coronaviruses have been known in human medicine for quite some time now. They are thought to be responsible for 10 to 30 percent of all adult respiratory diseases. Most are relatively easy to control. The SARS virus, which appeared overnight in 2002, was much more dangerous, as it can lead to acute lung failure. Around 80 percent of the SARS-CoV-2 virus's genetic makeup is identical to that of the first coronavirus. However, it probably invades human cells via additional portals of entry and is dissimilar in certain aspects of its envelope protein. The big difference between this and the earlier MERS and SARS pandemics is the speed at which the virus spreads. The global economy is far more connected than it was 10 or 20 years ago. SARS-CoV-2 has also been able to spread at such an incredible pace because it is more contagious than SARS. It already starts to multiply in the pharynx and is easily transmitted by droplets. Although the relative mortality of COVID-19 is lower than that of SARS, the exponential spread of SARS-CoV-2 means that the number of deaths cannot yet be predicted. This is why all measures are aimed to break

the chain of infections, protect the people who have not been infected, and slow the virus's spread to prevent the healthcare system from being overwhelmed. The public will have to follow basic hygiene and behavior recommendations such as social distancing rules and the like to achieve this goal. It is also essential to detect and quarantine infected individuals as soon as possible and to identify the people they have been in contact with in order to pinpoint and disrupt the chain of infection. And that requires far more people to be tested.

The data situation will have to improve, especially in regard to this last point. Researchers need enough valid data to draw on so they can make the forecasts that will underpin the planning of further steps to curb the spread of the virus.

2. Technical implementation by way of a corona tracing solution

The aim is to develop an IT system with digital tools to augment health authorities' practices and to help implement the corresponding recommendations of the Robert Koch Institute (RKI). This is to be done by way of a digital process that measures distance and time using Bluetooth technology on cell phones and notifies people who are at risk of a SARS-CoV-2 infection. The overall system's functionality derives from the legal mandate for public healthcare authorities. A thorough assessment has indicated this electronic tool has to meet the following prerequisites for deployment:

(1) The solution has to be elective; that is, entirely voluntary in terms of installation, de-installation and every element of use.

(2) Individuals tested for COVID-19 are to be informed of their test results quickly via a digital channel.

(3) Using Bluetooth technology on cell phones to measure time and distance, app users can be notified of an elevated risk of COVID-19 infection.

(4) Relevant information of purely epidemiological significance should be shared for research purposes.

(5) A data protection impact assessment (DPIA) describes data processing in compliance with data privacy regulations.

(6) A security concept is in place and the potential IT security risks and lines of defense have been mapped out.

Beyond that, the digital system should also provide pseudonymized data for epidemiological research, the goal being to improve the results achieved with this system.

Work on the German app commenced in early March 2020 at the participants' expense, with the support of base funding from the Federal Ministry of Education and Research (BMBF), and with a feasibility study funded by the Federal Ministry of Health (BMG). From the outset, this project was geared to create a pan-European solution that complies with data privacy laws. These goals were also stated later in the PEPP-PT initiative. French partners are on board to help develop the system. This cooperation with the Inria and Inserm research institutes was stepped up in recent weeks to achieve full

compatibility. The project's entire approach is underpinned by the conviction that the public healthcare system must retain sovereignty over the criteria for conducting risk assessments, recommending actions and sharing feedback within this type of system. The intention is to maximize support for the app on available devices by collaborating with the operating system vendors Google and Apple.

2.1 Function for messaging the apps of individuals who are at an elevated risk of COVID-19 infection

The proposed system comprises an app and a service on a server. The app is to be an automated tool to determine time and distance in exposure situations. Bluetooth technology on cell phones serves to measure time and distance. This will allow users to be apprised of an elevated risk of COVID-19 infection. The app augments German health authorities' procedures to make an important contribution as a digital tool. A key benefit of this system is that it detects the time and distance of exposure situations, which health authorities are unable to pinpoint with the procedures they follow today. These are encounters with people unremembered by or unknown to the individual who has tested positive, for example, fellow passengers on public transportation, patrons at the neighboring table of a restaurant, and so on.

Participation in this system and all its functions is entirely voluntary and requires the user's consent. Individuals who test positive can elect whether to share their epidemiologically relevant time/distance list in the app. Consulting the recommendations of the RKI for the given project, an affiliated service entity reviews the time/distance list to determine which apps are to be messaged to notify their users of an elevated risk of infection as determined by the measurement tool.

This is an analog to the health authorities' practice of interviewing a contact person and assessing their risk of infection. However, the service on the server has to assess the risk according to the RKI's recommendations, but based solely on the measurements taken and collected by the cell phone. The system thus supports the rapid detection and notification of possible contacts who are at risk of an infection. If the notified users behave responsibly, their actions can help disrupt the infection at the earliest opportunity. This is a key success factor in the effort to contain the COVID-19 pandemic.

This risk assessment based on cell phone data initially draws on the same science that underpins the health authorities' assessment practices. As it stands, potential exposure situations are limited to a distance of less than two meters over a period of more than 15 minutes. Data protection regulations prohibit this digital solution from asking any further questions. This is why the RKI's recommendation on the decision if and when app users are to be notified will have to be improved and adapted after the digital solution is rolled out, using the available data.

This will require models to simulate the pandemic's spread, an assessment of the system's functions, and the latest scientific findings to be factored into the equation and enriched with expert knowledge. These insights will underpin efforts to draft and implement the RKI's recommendations regarding the policy on notifying app users with an elevated risk of infection via the digital

system. As it stands, we believe these recommendations will have to be dynamic and adapted from time to time as the pandemic progresses and new information comes to light, for example, to adjust the timeframe for identifying pseudonymized close-range contacts.

2.2 Function for notifying individuals of their COVID-19 test result

The standard practice as described above is for health authorities to be notified of persons who have tested positive for COVID-19. The authorities then contact these individuals. The proposed system will also have to ensure that only those individuals who have tested positive actually provide their measured data to the service on the server to prevent it from working with incorrect data. A digital link to the diagnostic laboratories will be established for this validation process when the system is implemented. App users can voluntarily activate this notification option to get their test results quickly and directly. If an app user tests positive, no valuable time will be lost in the effort to contain the virus's further spread if he or she has enabled this messaging function that alerts other app users who are at an elevated risk of COVID-19 infection.

2.3 Data privacy

The proposed system does not collect or process data such as information about the place, phone numbers, names, and the like when the app is used. The use of the system via an installable app will be voluntary. Users may uninstall the app at any time without the service on the server being able to identify who deactivated the app. Registration does not require personal data such as the individual's name or phone number. A new independent identifier is created and assigned to the app to manage registered apps in an unequivocal way.

The cell phone sends bit sequences via Bluetooth to other cell phones within close range. Only valid for a short time, these bit sequences are derived from the random identifiers.

As it sends out these short-lived bit sequences, the cell phone also gauges the strength of incoming Bluetooth signals and estimates the distance to the source. The phone takes these measurements over a longer period, but stores only the epidemiologically relevant data in an encrypted format with the temporary bit sequences of the last 21 days. This process runs entirely in the background. It requires no user interaction unless a COVID-19-related event occurs.

If a user tests positive for COVID-19 and has given their consent, the process described above can be triggered to message the apps of individuals with an elevated risk of COVID-19 infection. Then the phone transmits the temporarily valid bit sequences it has stored and the associated measurements to the server in an encrypted format. The bit sequences are assigned to the apps' random identifiers. The decision to send a message to the respective apps with the random identifiers is made based on the RKI recommendations described above.

The system helps the RKI and the health authorities carry out their assigned duties. The recommendations on which these tasks are based will have to be adapted time and again to the latest

scientific insights. This is why, ideally, the appropriate government authority will operate the service and host server in keeping with its responsibility to uphold data protection laws. The system serves the sole purpose of combating the COVID-19 pandemic. The service will be shut down if it is no longer needed or effective as a digital tool to augment the work done by health authorities.

The design of the cryptographic data protection protocols has been documented and published on GitHub. The data protection concept and data protection impact assessment are being finalized. The app and service code will be made available as an open source project on GitHub. Under the statutory responsibility set out by German law, the system could be operated by the RKI, for example. The system's design factors in the principle of data minimization in keeping with data protection regulations.