Issue 1 | 2020

EDPS

TECH DISPATCH

Contact Tracing with Mobile Applications

In public health, contact tracing is the process to identify individuals who have been in contact with infected persons. Proximity tracing with smartphone applications and sensors could support contact tracing. It involves processing of sensitive personal data.

I. What is Contact Tracing?

During epidemics of infectious diseases, such as the Coronavirus disease (COVID-19), it is important to lower the number of new infection cases and to stop it eventually. Therefore the infection chain of onward transmissions must be interrupted. When those persons known to be infected reveal their recent contacts, other infected persons may be identified, informed and e.g. isolated already early on, even before they become aware of their infection. **The process to identify contacts of known cases is called contact tracing**.

A person becomes a *contact* of a primary case by e.g. face-to-face contact within a short distance over some time span, physical contact or spending time indoors together–all within the incubation period of e.g. up to 2 weeks for the coronavirus disease.

To establish the risk exposure in contact tracing, information about the **distance** between the persons and the **duration** of contact are important. *Close contacts* with high-risk exposure may then become subject to different rules or treatments.

I.1. Traditional Contact Tracing

After a confirmed or probable case of an infected person has been identified, health authorities usually **interview the person, e.g. by phone**. The European Centre For Disease Prevention and Control (2020) lists the following generic steps:

1. The person's clinical history is collected.

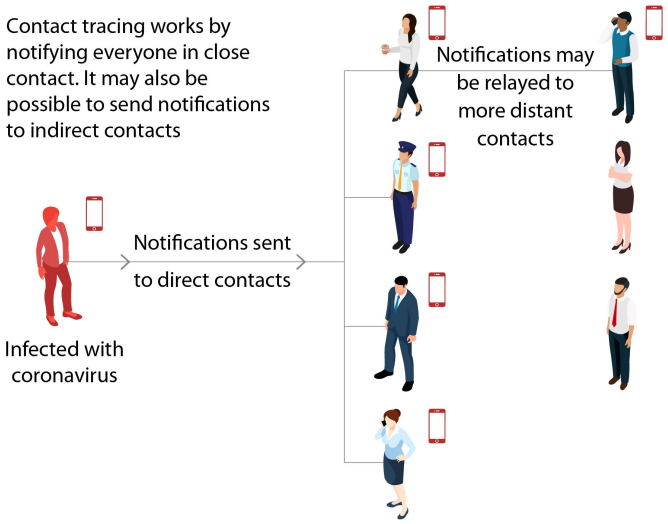

Figure 1: Contact Tracing.

2. The contacts of the identified persons are gathered with their risk of exposure for classification, and background data like e.g. work with vulnerable populations.
3. The contacts are then called to confirm their health status and to test those with symptoms, monitor actively close contacts, and ask other contacts to self-monitor and apply precaution.

This case-by-case approach is very resource intensive. Tracing all contacts can be difficult when people have many contacts, do not accurately remember them or cannot provide information on how to reach out to them.

I.2. Digital Proximity Tracing

To **support and complement** traditional contact tracing, radio wave sensors built into smartphones could be used because they can **automatically detect close contacts**: the smartphone could be used to record when two people are in close enough proximity for long enough that there is a high risk of contagion if one of them has e.g. the coronavirus.

Smartphones can be equipped with new functionalities, with the installation of a **dedicated smartphone application** and/or operating system software update, empowering their holders via the smartphone sensors to log preventively with little or no personal effort a list of proximity contacts even *before* a suspicion of an infection emerges.

The **efficiency** of such *digital proximity tracing* is actively being researched. Early results are optimistic if other conditions, such as infection testing capacities and broad technology adoption, are also guaranteed (Ferretti et al. 2020). Digital tracing could be particularly useful when people may have been in touch with many contacts during longer periods of symptom-free contagion, who would otherwise be hard to recall afterwards.

With ***global navigation satellite systems*** like GPS or Galileo, smartphones can determine their geographical location with up to 5 m precision outdoors. If smartphone holders upload their locations to a central service, e.g. of a health authority, their proximity contacts can be computed. Proximity tracing in e.g. shops or public transport is not possible.

With ***Bluetooth Low Energy*** **(BLE) technology**, smartphones broadcast messages with small data packages to their close environment, typically in between a few and hundreds of meters. Modern smartphones permit applications to configure the broadcast range, e.g. to limit it to the nearest few meters. Such messages may contain a smartphone identifier and application-specific data (the *payload*). Other smartphones with support for BLE and within the broadcast range can detect these messages.

If the BLE payload is used to recognise smartphone holders, other peoples' smartphones can register them automatically as BLE proximity contacts. When smartphone holders are later confirmed to be infected (e.g. by their doctor), they then can choose to upload contact tracing data to a central service. Depending on the contact *matching* approach, this service can then either notify contacts about their risk exposure directly (*centralised* matching) or publish data, so contacts can compute their exposure themselves with their smartphones (*decentralised* matching shown in Figure 2).

Figure 2: Digital Proximity Tracing.

The ***Wi-Fi*** interface of smartphones also allows to broadcast radio waves with identifiers, but is not very energy-efficient and therefore less appropriate for a functionality to be active non-stop on battery-powered devices.

II. What are the data protection issues?

Both traditional and digital proximity contact tracing involve the **processing of personal data**. Where the data relates to infected persons, it is **health data** requiring special protection.

II.1. Large scale surveillance

Digital proximity tracing raises novel data protection risks as it provides for **preventive, contact recording of a very large number of the population in public and private spaces** using radio wave signals invisible to human eyes.

Contact tracing applications are therefore likely to result in a high risk to the rights and freedoms of natural persons and to require a **data protection impact assessment** to be conducted prior to their deployment.

II.2. User identification

The contacts of a case may include family members, neighbours, or colleagues from work. Linked to other data, e.g. from social networks, it is technically possible to learn the name of the infected person, the place of residence and work and a number of other activities and potentially their location. The number of contacts and their frequency may even reveal **social habits**, such as religious practices. Linking with location data, as it happens with GPS-based tracing, could allow to infer a detailed picture of the daily routine.

Data minimisation and **privacy-enhancing technologies** can therefore prevent harm through identification of contacts and infected cases.

As tracing apps can function without direct identification of their users, appropriate measures should be put in place to **prevent re-identification attacks**.

As **location data** are prone to re-identification, location-based tracing is best avoided at all. Digital proximity tracing smartphone applications (the *tracing apps*) do not require tracking the location of individual users. Instead, **proximity data** should be used, specifically information obtained via the use of Bluetooth BLE.

Tracing apps can employ **pseudonymous identifiers** for proximity contacts and change them periodically, for example every 30 minutes. This reduces the risk of data linkage and re-identification. *Secret Sharing Schemes* allow to split identifiers in parts and spread their broadcasting over a given timespan. Adversaries attempting to reveal and map contacts would need to wait to receive the minimum number of parts required to reassemble the identifier again.

The service providing testing and confirming the infection status can operate **independently** from the central service to which the cases upload contact tracing data to prevent linking of contact tracing data to medical case files. To still ensure that data is only uploaded by confirmed cases, the central service could require a digital proof.

II.3. Data protection by design

With **centralised matching**, upon app installation users register at the central service (Inria and Fraunhofer AISEC 2020). Once individuals are confirmed to be infected, they can choose to upload their recorded contacts to this service. Then, the service can match the uploaded contacts to registered users and send them a notification about their risk exposure. Notified users do not learn any details thus protecting the privacy of the confirmed cases.

With the pseudonymous contact data received in this process, the central service could possibly also compute infection chains and the network of contacts of all cases. While this infrastructure and this data are likely relevant to study and contain epidemics, it may therefore also allow for **large-scale behaviour monitoring**. The service poses a single point of failure. Without it, users cannot register or even continue tracing. Hence, such a service needs to implement extraordinary organisational and technical data protection and cyber security safeguards to build user trust.

With *decentralised matching*, **tracing app users do not need to register** after the app installation. The keys used to generate pseudonymous identifiers for broadcasting are managed locally on their smartphone (DP-3T Project 2020a). Once app users are confirmed to be infected, they can choose to upload their keys. All tracing apps download regularly public updates with keys of recent cases. The smartphone computes matches locally with the recorded contacts and generates accordingly notifications of risk exposure.

Unlike in the case of centralised matching, the keys of recent cases with confirmed infection are publicly distributed. Adversaries may link them with previously recorded location and timestamp data to identify and map infected cases. Though, covering significant areas would require many sensors.

Data protection risks remain with centralised and decentralised matching. While centralised matching assumes trust in one central service, decentralised matching assumes trust in each individual to not engage more into radio data collection and correlation than what is necessary.

II.4. Purpose limitation

In the context of a tracing apps, careful consideration should be given to aspects of purpose limita-

tion and storage limitation, i.e. determining in advance for which specific purposes (such as contact tracing and/or scientific research) the personal data may be used, and by whom and for how long it may be stored.

Once the epidemic has stopped, and **contact tracing apps are no longer needed**, a procedure must be put in place to stop the collection of identifiers (global deactivation of the application, instructions to uninstall the application, automatic uninstallation, etc.) and to delete all collected data from all databases (mobile applications and servers).

II.5. Lack of transparency

Tracing apps may only achieve their maximum efficiency if used by the largest possible share of the population. Lack of explanations on how the tracing apps work and how they protect the user's privacy might create a lack of trust. Therefore the use of tracing apps should be **voluntary and transparent** to the user. The collected information should **reside on the user's smartphone**.

II.6. Insufficient data accuracy and integrity

Radio wave transmission follows different principles than transmission of infections. Unlike radio waves, infections cannot be transmitted through windows or walls. Radio waves cannot track other interaction aspects like the ability to touch contaminated surfaces or shake hands. Moreover, sensors can only detect other sensors of their kind and do not detect contacts without a suitable smartphone. In consequence, digital proximity tracing is prone to record contacts with false positives and false negatives.

II.7. Security of personal data

The use of radio wave signals may also cause issues for the **security and integrity** of the system. In principle, adversaries can employ more powerful radio antennas to either send noise and block radio transmission in the environment, or broadcast their own or relay others' pseudonyms in a much larger area. The former distorts the quality of service (denial of service). The latter leads to false risk notifications when these recorded proximity contacts are notified as infected at a later stage without actual proximity in the past. Adversaries can also attempt to reveal infected people by moving around to capture radio signals and map the location of detected proximity contacts that may later be or are already notified as infected.

To enable all actors involved in the development and operation of contact tracing apps to **comply from the onset with EU data protection laws**, the European Data Protection Board (2020) and the European Commmission (2020) have published detailed guidance.

Recommended Reading

DP-3T Project (2020a). *Decentralized Privacy-Preserving Proximity Tracing: Whitepaper*.

– (2020b). *Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems*.

Bock, Kirsten et al. (2020). *Data Protection Impact Assessment for the Corona App*. Version 1.6. FIfF.

European Centre For Disease Prevention and Control (2020). *Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union*. Technical Report.

European Commmission (2020). *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01*. C(2020) 2296 final.

European Data Protection Board (2020). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*.

Ferretti, Luca et al. (2020). *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing*. In: *Science*. ISSN: 0036-8075. DOI: 10.1126/science.abb6936.

Inria and Fraunhofer AISEC (2020). *ROBust and privacy-presERving proximity Tracing protocol*.

Privacy International (2020). *Bluetooth tracking and COVID-19: A tech primer*.

This publication is a brief report produced by the Technology and Privacy Unit of the European Data Protection Supervisor (EDPS). It aims to provide a factual description of an emerging technology and discuss its possible impacts on privacy and the protection of personal data. The contents of this publication do not imply a policy position of the EDPS.

Issue Author: Robert RIEMANN,
Lukasz OLEJNIK
Editor: Thomas ZERDICK
Contact: techdispatch@edps.europa.eu

To subscribe or unsubscribe to the EDPS TechDispatch publications, please send a mail to techdispatch@edps.europa.eu. The data protection notice is online on the EDPS website.

ISSN 2599-932X
HTML: ISBN 978-92-9242-429-9
QT-AD-20-001-EN-Q
data.europa.eu/doi/10.2804/336130
PDF: ISBN 978-92-9242-430-5
QT-AD-20-001-EN-N
data.europa.eu/doi/10.2804/45722