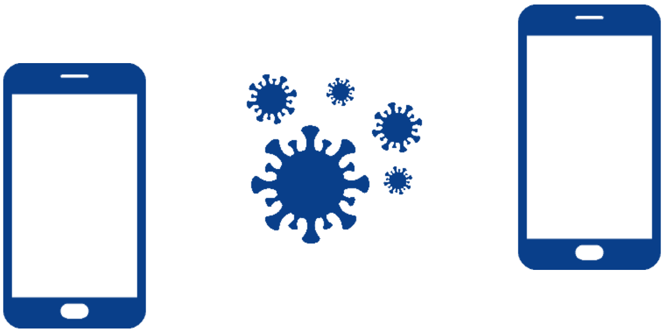
CONTACT TRACING APPS FOR COVID-19

Repository of Basic Technical Terms for Public Health Professionals



JULY 2020

The Association of Schools of Public Health in the European Region (ASPHER)

TABLE OF CONTENTS

AUTHORS:

Tobias Weitzel, Department of Public Health, University of Copenhagen
tobias.weitzel@outlook.com

Henrique Barros, Institute of Public Health, University of Porto
hbarros@med.up.pt

1. CONTACT TRACING APPS – GENERAL TERMS

Contact Tracing App	Contact tracing apps are a supplementary method of contact tracing that relies on the functions and features of mobile devices (phones) to determine contact between an infected individual and others. The two most common approaches used to support manual contact tracing are proximity tracing and location tracking.
Central Backend Server	A central backend server offers a broad range of functions for programs and devices. For example, storing user data or performing centralised processing of data. All contact tracing apps have a central backend server, which supports the functioning of these apps.
Local database	In the context of apps, a local database exists only on the respective phone and not on central backend servers. Data that is used by contact tracing apps (such as location history) is stored in a local database on the phone.
Platform Support	In the context of apps, this refers to the ability of an app to run on a specific platform. A contact tracing app should be supported on both iOS and Android and have reasonable backwards compatibility for older versions.
Interoperability	Interoperability is the ability of a contact tracing app to transfer data between different information systems and public health entities. Cross-border inter-operability is the flow of data and information exchange between countries that use different apps.
Localisation	Localisation is the adaptation of an app to fit a specific cultural context, including language and correct time formats. A contact tracing app should be available in the languages most commonly spoken in a country – not just the official languages. Some contact tracing apps have the same developer, but the respective content is localised for multiple countries. For example *StopKorona!* for North Macedonia and *VírusRadar* for Hungary.
Source Code	A source code is a collection of human-readable codes, sometimes with comments, created by a programmer. They specify actions to be performed by a computer program (such as an app).
Open Source	In this context, open source refers to the availability of the source code of a computer program to the public. The source code of many contact tracing apps is available online to ensure transparency and allow for other use and modification.

2. PROXIMITY TRACING VIA BLUETOOTH LOW ENERGY

Proximity Tracing	Proximity tracing uses Bluetooth Low Energy (BLE) signals to determine whether two phones were close enough for their users to be exposed to each other.
(Classic) Bluetooth	(Classic) Bluetooth is a wireless technology that is used for exchanging data between mobile devices over short distances. It uses short-wavelength radio waves.
Bluetooth Low Energy (BLE)	BLE is a variant of classic Bluetooth that aims to provide similar capabilities but at significantly lower power consumption. It is used for applications that do not exchange large amounts of data. BLE is used by many contact tracing apps due to several reasons: **(1)** BLE is supported on most phones. **(2)** BLE consumes less energy that other forms of wireless communication. **(3)** BLE can be used in a way that preserves privacy.
Bluetooth Low Energy Beacon	A BLE beacon is a radio transmitter that repeatedly broadcasts to other nearby BLE-enabled devices. It allows BLE-enabled devices to exchange data when in proximity to each other. The physical range is typically less than 10 meters, which makes it unlikely that information is sent beyond this range. This function is used by several contact tracing apps to transmit information to all nearby phones which also use the respective contact tracing app.
Application Programming Interface (API)	An API is a set of callable function and procedure signatures which allow interactions between multiple software components – a way of different programs and systems to interact and work together. APIs facilitate the access to features and data from various software components, libraries, and platforms. This access is enabled at different levels of the software stacks such as operating systems or applications.
Google Apple Exposure Notification	Google and Apple have jointly created an API ("Exposure Notification") to enhance BLE features and functions for official contact tracing apps. The aim of their collaboration is easing the implementation of the respective contact tracing apps and their interoperability across their smartphone operating systems iOS and Android. Most of this section is based on the Google Apple API.
Temporary Exposure Key (TEK)	The TEK is a unique key that is independently and randomly generated on each phone with a BLE-based app (see "Cryptographic key" in section 5). The TEK is generated once every 24 hours and usually remains on the phone for up to 14 days.
Ephemeral Identifier / Rolling Proximity Identifier	Both terms refer to random proximity identifiers derived from the phone's TEK. These identifiers are shared between two BLE-enabled phones to determine if they were in proximity for exposure of their users. A new identifier is usually generated multiple times per hour (for their privacy aspects, see "Cryptographic Key" in section 5).

Diagnosis Key	The Diagnosis Key refers to a set of TEK (usually from the past 14 days) of an infected user, who reported their infection via the app. Diagnosis keys are shared with a central backend server and then distributed to phones with the app, which use them to check for exposure (see centralised / decentralised matching below).
Proximity History	A BLE-based app creates a local database with all anonymous identifiers received from phones that were in close proximity. The data is stored for a set period of time, which usually corresponds to the incubation period of the virus.
Received Signal Strength Indicator (RSSI)* *not unique to Bluetooth technology	RSSI is a measurement of the strength of a received signal at the receiving device. BLE can measure the strength of a signal received from another device. In theory, the signal strength is proportional to distance between two devices. However, the signal can be affected by physical obstacles and surfaces around the device, e.g. walls, human bodies, pockets, and purses. RSSI can indicate a possible contact between users: Strong signal indicates close proximity and potential for transmission of the virus; a weak signal indicates the phones were not close enough for transmission.
Exposure Risk Calculation	This calculation refers to the process whereby the level of risk of exposure is determined by an app using the RSSI and other parameters, such as duration of contact. Each contact tracing app may use different epidemiological heuristics, thus parameters differ across apps.
Centralised matching	Centralised matching is an approach whereby a reporting user informs the app of their positive testing and the app uploads their diagnosis key and proximity history to a central server. The central sever then associates this data with contacted users and alerts those users.
Decentralised matching	Decentralised matching is an approach whereby a reporting user informs the app of their positive testing and the app uploads their diagnosis keys to a central backend server. The central backend server then sends their diagnosis keys to other users' apps which locally determine whether an exposure event has taken place.
Exposure Alert / Exposure Notification	Based on matching processes to determine proximity, users will receive an exposure notification after they have been exposed to an infected user. They often trigger a follow up, such as a recommendation to get tested.

3. LOCATION TRACKING VIA GPS, IPS AND QR CODES

Location Tracking	Location tracking is an approach that employs technologies that physically locate and track the movement of people. It matches the location of phones of infected persons to the phones of people in their vicinity. Some contact tracing apps utilize GPS, IPS or QR Codes for location tracking.
GPS	GPS commonly refers to navigation systems that use satellites to provide geo-spatial positions. These systems allow mobile devices, such as phones, to determine their location within a few meters. However, GPS is mostly limited to outdoor positioning as the GPS signal is too weak to render reliable (if any) indoor positioning results. Some contact tracing apps access GPS location data of phones.
Indoor positioning system (IPS)	IPS is a network of different technologies which determine indoor positioning. It is used where GPS is inadequate, such as inside multi-story buildings or underground locations. A common IPS design is determining the distance to nearby Wi-Fi access points or Bluetooth Beacons by measuring the intensity of RSSI (see “RSSI” in section 2). In some GPS-based contact tracing apps, Wi-Fi location data is collected to increase the accuracy of location tracking.
QR Code	A QR code is a type of barcode in a square pattern. It contains information about the object it is attached to. Some contact tracing apps have a function that allows users to scan QR codes to log the places they have visited. A necessary condition for this approach is the presence of unique QR code posters in many public locations.
Cell Site Location Information (CSLI)	CSLI are records stored by telecommunication operators that are collected each time a phone connects to one of their cell towers. They record the exact time and duration of each connection. The location of a phone can be narrowed down to somewhere in the reception zone of the respective cell tower. For urban areas with a high intensity of cell towers a technique called “triangulation” can be used to estimate the location precisely. Rural areas may see several kilometres between cell towers and therefore determining locations is less precise. Their use in contact tracing apps is limited.

4. GDPR LEGAL TERMS

General Data Protection Regulation (GDPR)	GDPR is the data privacy and security law of the EU and the EEA. This law imposes obligations onto organizations anywhere when they target or collect data of people in the EU or EEA. Contact tracing apps in the EU and EEA must conform to GDPR.
Personal Data	The GDRP has a broad conception of personal data, defining it as any information which is related to an identified or identifiable natural person. Examples for personal data are name, home address, email address, ID numbers, location data or internet protocol address. The GDPR also includes provisions for "sensitive personal data", such as health-related information, which requires special protection. Contact tracing apps involve the processing of personal data, in particular sensitive health-related information, for example data relating to infected users. The collection of location data (with GPS for example) is problematic as it is prone to re-identification.
Pseudonymisation	Pseudonymisation is the process of removing identifying information from personal data, so that it can no longer be attributed to a specific person without the use of additional information. This additional information should be kept separately and is subject to technical and organisational measures to keep it secure.
Data Collector and Data Processor (GDPR)	The **data controller** determines the purposes for which and the means by which personal data is processed. The **data processor** processes personal data on behalf of the data controller. In some cases there is one entity which is both data collector and data processor. For many contact tracing apps, public health authorities are the controller and processor of the app data. They determine the purpose and means of the contact tracing app and also process the data.

5. CRYPTOGRAPHY

Cryptography	Cryptography is the practice of securely transmitting and processing information through the use of codes, most commonly in the form of mathematical algorithms. It is based on the encoding of plaintext into a text that is unreadable by a human or a computer (so-called "ciphertexts"). To ensure that personal data from contact tracing apps is rendered anonymous, cryptographic functions are implemented in those apps to generate and process pseudonyms (see "Pseudonymisation" in Section 4)
Encryption and Decryption Process	**Encryption** is the process of encoding a plaintext into a ciphertext. **Decryption** is the reverse process, decoding of a ciphertext into the original plaintext. To ensure messages are encoded and decoded correctly, the same cryptographic key must be used in both processes.
Cryptographic Key	A cryptographic key is a string of characters used to specify the transformation of plaintext into unreadable "ciphertext" and vice versa. In BLE-based apps, a cryptographic key, the TEK, is used to generate random proximity identifiers (see "Ephemeral Identifier / Rolling Proximity Identifier" in section 2). These identifiers are only "readable" with the respective TEK. From the identifier alone it is not possible to identify the phone which originated it. A simplified example of how cryptography is used in proximity tracing: **(1)** The TEK is generated using a cryptographic random number generator (see "Temporary Exposure Key" in section 2). **(2)** Proximity identifiers are derived cryptographically from the TEK. **(3)** Encrypted proximity identifiers are broadcast to other phones close by which store them in a local database (see "Proximity History" in section 2). **(4)** If a user tests positive, their relevant daily TEKs (as diagnosis key) can be uploaded to a central backend server (see "Central Backend Server" in section 1), which then shares it with the apps of other users. **(5)** On other apps, the diagnosis key is used for matching against the collected proximity identifiers in the local database.

6. PRIVACY-ENHANCING TECHNOLOGIES

Privacy-enhancing Technologies (PET)	PET are a group of technologies that enable analysis and insights from data without requiring the sharing of the underlying data itself. A decentralised system for contact tracing apps leaves health authorities with limited insight into population-aspects of the virus, e.g. geographic hot-spots, rate of spread. PET could be used to ensure that individuals can report their health data in an encrypted manner, allowing health authorities to gain insights into population-aspects while privacy is preserved.
Differential Privacy	Differential privacy refers to an aggregation of data which includes randomly generated noise. This noise limits each party's ability to trace back individual inputs. Differential privacy is normally used in anonymous statistics, such as mobility reports, which help health authorities to make critical macro-level decisions to fight the coronavirus. The application to a contact tracing app is limited because it does not generate individual precise results.
Homomorphic Encryption	With homomorphic encryption, data is continuously encrypted: while resting, in transit and in use. This allows an untrusted third party to perform computations on encrypted data without knowing the plain text. Only the owner of the data can decode and learn the analysis result. The untrusted party cannot learn any relevant information or plain text as the results are always returned as encrypted data. Problems of homomorphic encryption: **(1)** It is very slow in performing simple processes, as it takes more computer power to process encrypted data whilst keeping it encrypted. **(2)** Current methods/technologies are still slow and inefficient for any practical application with real time requirements. Homomorphic encryption can enable public health authorities to gain insights into population health information from contact tracing without exposing sensitive health information.