COVID-19

Digital Contact Tracing Applications

June 2020

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

Table of Contents

Introduction

Purpose and audience

As the world works around the clock and across many fronts to combat COVID-19, the mobile industry is playing a critical role. Mobile network operators (MNOs) are providing robust and secure connectivity for individuals, business continuity and government response.

To support the efforts across one of those fronts, this paper presents current and pertinent information about digital contact tracing applications (apps), with a focus on aspects that have been discussed widely and intensively in recent weeks, and which are of most relevance to MNOs. In this context, the majority of this paper covers Bluetooth-based apps, rather than GPS-based apps, and aims to explain the background and facilitate the forming of fact-based opinions.

While the primary audience is MNOs, this paper can be shared with other stakeholders where deemed useful for discussion.

Introduction to contact tracing

Contact tracing is a longstanding tool used for epidemiological investigations which can help reduce infection rates in a targeted way and with less impact on the overall economy compared with lockdown approaches[1]. Traditional methods for contact tracing are labour-intensive and hard to scale up to meet the demands of COVID-19. Consequently, a number of digital contact tracing apps are being developed and used.

Digital contact tracing apps are typically used to trace the locations, or proximity between, pairs of people who have the app installed and active on their smartphones. If an individual with the app on their phone is infected with the COVID-19 virus, the app enables others who were in close contact with that individual in the recent past to be notified about a potential infection risk and to take appropriate action.

This document provides a background and summary overview of the main types of digital contact tracing currently being considered in the context of COVID-19, highlights some of the key issues and explores how mobile operators could help.

Note:

- This paper does not cover all implementations of contact tracing apps but focuses on those currently most popular.

[1] In an epidemiological setting, contact tracing involves identification of people who may have come into contact with an infected person (i.e., ‘contacts’) and subsequent collection of further information about these contacts, so that they can be tested for infection. Contact tracing may be voluntary or mandatory, depending on local legal frameworks.

- It is important to note that mobile operator cell tower location data is not typically used for digital contact tracing apps and whilst other sources of radio signal, such as WiFi, could in theory be leveraged to provide location or proximity of people, these have not currently gained traction and are not covered in this paper.

- There are also digital contact tracing solutions, which do not (or not mainly) rely on smartphone apps but on a central collection of location data (e.g. from point-of-sale credit card payment transactions, surveillance cameras and similar). This paper does not cover such approaches.

Limitations of digital contact tracing apps

It should be noted that digital contact tracing apps are not always the best or only solution. In some countries, the lack of smartphones or availability of 3G/4G networks mean that apps are not a viable medium. In countries with higher smartphone penetration and more advanced networks, apps may still not be adopted in sufficiently high numbers to be useful and will only be of value if combined with a suite of other government or healthcare policies e.g. rigorous and widespread testing.

Contact Tracing Apps

Main types of digital contact tracing apps: Location VS proximity

Apps typically fall into two camps, those that use location data and those that use proximity data.

(1) **Location –** typically collected from the GPS signal of the user's device, giving the longitude and latitude coordinates of the device over time.

Example – Safe Paths from MIT.

Note: Whilst some countries have used a variety of sources to collate location traces of individuals e.g. GPS, MNO network cell location and CCTV / surveillance cameras, this is not widespread and most apps rely on GPS data alone.

(2) **Proximity** – this approach traces the close proximity of pairs of people irrespective of where the proximity takes place. The most common approach is to measure the signal strength of Bluetooth signals from pairs of devices when the users are in close contact and without any knowledge of the geographic location.

Example – TraceTogether in Singapore.

Examples of hybrid location / proximity apps include Care19 used in North Dakota, USA, and Smittestopp in Norway. Both apps utilise Bluetooth and GPS data.

Privacy aspects of location and proximity apps

Protecting the privacy rights of users is a key priority for the mobile industry. Information about the location and proximity of mobile users should be safeguarded, and users should be able to make choices about how their data is shared, and be provided with information about how their data is used and protected.

(1) **Location** – privacy may be hard to preserve in GPS-based apps (unless the app itself stores and analyses data on the user device, which helps mitigate privacy risks). The disclosure of an individual device location over time has potential for the re-identification of that individual. Knowing a short history of someone's whereabouts provides more insight into their private lives than the mere disclosure of anonymous codes that can facilitate a message to users that have been near the infected user.

(2) **Proximity** – to address data privacy in Bluetooth-based apps, most of these solutions only disclose a randomly-generated anonymous code that changes regularly, e.g. daily. In this way, the personal identity of the user of the sending device is not disclosed and it is also not possible to link the anonymous codes to a single device.

The anonymous codes received from the various sending users' devices are kept on the recipient device in encrypted form and are inaccessible to the recipient user. If the recipient user subsequently receives confirmation of a positive COVID-19 test result, a representation of the anonymous data on their device is uploaded to a server (initiated by that user with their consent), which allows other devices that have been in close enough contact, for a long enough duration over a preceding number of days, to make their users aware of a potential risk.

Bluetooth-based proximity apps: Centralised vs decentralised

There are two variations of the Bluetooth-based approach, often labelled "centralised" and "decentralised".

(1) **Centralised approach** – when a user receives confirmation of a positive test result, they can upload the list of anonymous codes stored on their device to a central server belonging to the end-to-end solution (typically controlled by the government or the national health authority). This enables the server to "match" the anonymous codes of people at risk and notify the relevant users.

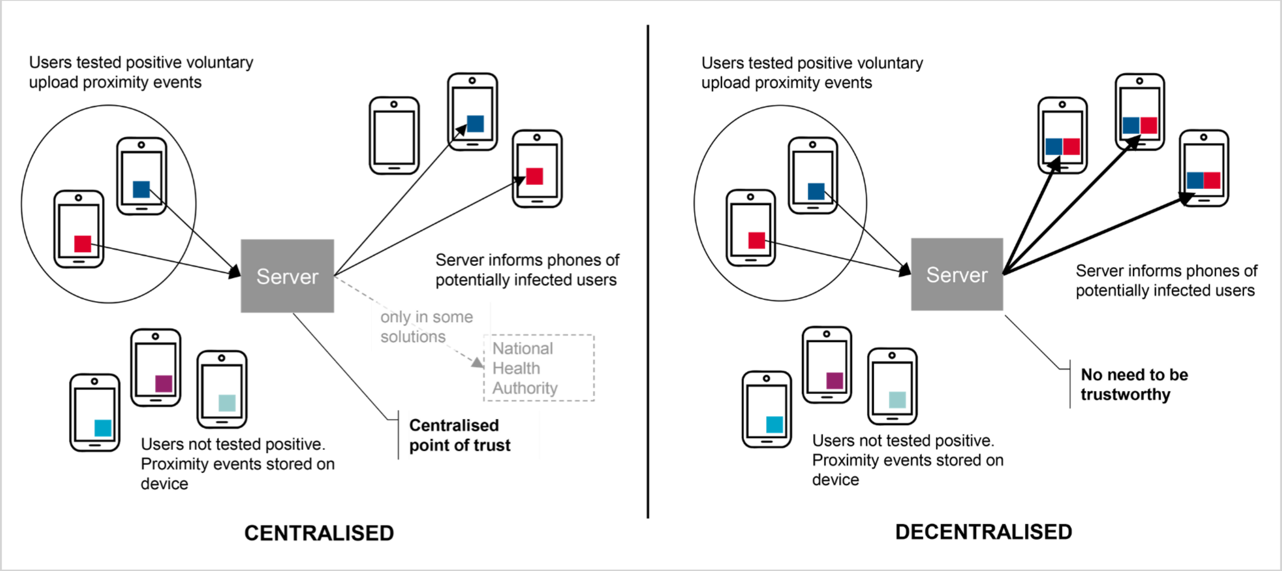
Example – TraceTogether in Singapore.

- Some centralised solutions only deal with pseudo-anonymous identifiers and inform people at risk directly through the digital solution e.g. the PEPP-PT initiative

- Some solutions are aware of the app users' wider personal information and inform people at risk through other means. National health authorities may step into direct contact with these people e.g. COVIDSafe in Australia

(2) **Decentralised approach** – the anonymous codes are still sent to a central server, but the system merely distributes out the codes indicating devices of people who have tested positive for COVID-19 which are then sent to or downloaded by all other phones. The code-matching process executes only on the phones in this decentralised model, requiring the user to download the data periodically e.g. daily to find out if they might have an infection risk due to being in proximity with an infected person.

Example – the DP-3T initiative


Users tested positive voluntary upload proximity events
Server
Server informs phones of potentially infected users
only in some solutions
National Health Authority
Centralised point of trust
Users not tested positive. Proximity events stored on device
CENTRALISED
Users tested positive voluntary upload proximity events
Server
Server informs phones of potentially infected users
No need to be trustworthy
Users not tested positive. Proximity events stored on device
DECENTRALISED

Summary of key differences

	Centralised	Decentralised
Matching of infected user with those in recent proximity	Matching takes place on server	Matching takes place on device
Information held on the data server	The solution assigns each handset a persistent identifier that is used to create anonymous ephemeral IDs (EBIDs) for the device that change at regular intervals. These are created by encrypting the president identifier with a global broadcast key via the backend server. EBIDs are broadcast via Bluetooth by the phone, and the EBIDs of other phones in close proximity are recorded. If a patient tests positive for COVID-19, with their consent the app uploads all EBIDs recorded over the prior 3 weeks to the server, with time of contact. The server uses the global broadcast keys to decrypt the IDs, revealing the persistent identifier (i.e., the pseudo-anonymised identity) of all the devices that were close to the infected person over a certain time frame.	Server is never aware of any critical information (i.e. device encounters). This information is stored on the device app. The server has less knowledge because it holds only the data indicating which anonymised identifiers correspond with COVID-19 positive status.

Data volume communicated between phones and server	Data volume is very small.	The server needs to send all data of the anonymous IDs of COVID-19 infected persons to all other phones for evaluation, resulting in a data volume which is significantly larger than in the centralised approach. The amount of data might become critical from network capacity perspective and/or for the users as it could result in cost for them. Data consumption scales with number of new infections per day and number of overall participating people. So, in particular for bigger countries, in the case of a next significant infection wave, this might become a challenge.
Privacy, security & trust	The backend server creates the EBIDs (via the global broadcast key), and the EBIDs are linked to the persistent identifier, which means that the backend server has information about that pseudo-anonymised user's proximity contacts, which could be compared to 3rd party data to reveal an individual's specific identity. Security of the backend server and trust in the party controlling it are key.	The decentralised model does not include a backend server that could be used to link ephemeral IDs to a persistent device ID. Re-identification risks could remain, though. From a trust perspective the backend server is not critical. The security of the devices, the operating systems and the proximity tracing application software are key, as well as trust in the parties providing these elements. The same holds true for the centralised approach of course.

Other challenges

There are a number of challenges which need to be successfully addressed in order to result in a significant positive impact on the control of the COVID-19 pandemic. At the highest-level, any contact tracing effort – digital or manual – relies on testing. For proximity-based contact tracing apps to be effective, health authorities should be conducting infection tests at high-volumes. The proximity approach will not be effective if only a small fraction of infected people are identified by testing. The widespread availability of infection testing will likely impact whether people act on any proximity-based notification of possible infection. If a testing programme cannot accommodate people seeking tests based on proximity-based notifications, user interest in testing may wane, diminishing the utility of the app.

There is also the general question of how to ensure the efficacy of the app if the app is not downloaded by the majority of the population. To be effective, more than 50% of the population must download and use the app, without fragmentation. How will health authorities and others encourage people to opt-in? Some governments have considered mandating the use of these apps, but the possible mandated use of contract tracing apps has been met with resistance. To ensure high-levels of participation, there must also be high-levels of trust, reinforcing the importance of user privacy and security.

Addressing the efficacy of the app also requires consideration of the proper epidemiological interpretation of proximity measurement, e.g. determining the risk level of infection based on proximity events. The distance and duration of proximity events will impact the effectiveness of the app. Whether the proximity event occurred indoors or outdoors will also impact efficacy.

There are also a number of technical and usability issues to consider. For the app to be widely-adopted, it must not negatively impact or create interference with other apps, or the battery, given that constantly monitoring Bluetooth radio could drain the phone battery. There must be no adverse impact with other Bluetooth services, e.g., headphones, or car-pairing.

There are also issues related to the interoperability of the app across the array of mobile devices. Devices with different technical characteristics (e.g. chip sets, antenna) need to be considered when deriving precise proximity measurements based on radio signal strength. Additionally, a Bluetooth-based solution will not be successful in every market, because it is questionable if the required Bluetooth capability can be retrospectively applied to non-smartphone devices. Apple and Google are working collaboratively on updates to the iOS and Android platforms to heighten privacy and reliability of existing Bluetooth capabilities (Low Energy Beacons) used for this solution, but the same may not be available on other platforms.

There are also potential impacts on mobile networks, depending on the model underpinning the app. A decentralised model could require a volume that could be so high as to impact networks. It could also result in bill shock for customers. In realistic scenarios (e.g. based on projected numbers of infections per day, in a highly populated country), the decentralised approach could require hundreds of megabytes of data per user, per month.

Data privacy and trust

The GSMA recently issued COVID-19 Privacy Guidelines, articulating the mobile industry's best practices for responsibly leveraging mobile big data to address the pandemic. These guidelines address the mobile data that is under the control of MNOs, i.e. metadata, non-identifiable aggregated data and insights. MNOs do not have control or visibility of data collected, processed and stored on third party apps.[2] MNOs also typically do not play a direct role in any proposed COVID-19 location tracing or proximity tracing app. Nonetheless, MNOs promote the implementation of privacy best practices, such as the GSMA Mobile Privacy Principles and Privacy Design Guidelines for Mobile App Developers.

There are different data protection frameworks guiding the development of location tracing and proximity tracing apps. In the EU, where mobile apps have been identified as part of the pandemic exit strategy, the General Data Protection Regulation regulates the collection, processing and retention of all personal data.

The ePrivacy Directive regulates the collection of information from terminal equipment, including mobile devices. Guidance from the body of European Data Protection Authorities – the European Data Protection Board – clarifies that contact tracing apps, including both centralised and

[2] Unless the app was developed by the mobile network operator, for example, an app to provide users with billing information.

decentralised Bluetooth proximity-based models, can comply with EU law, provided various conditions are met. This reflects that data protection can coexist with digital contact tracing.

However, despite these legal clarifications, the centralised proximity tracing model has met with significant criticism from privacy advocates and other stakeholders in the tech community who believe that the centralised model provides governments with information they could use to attempt to reverse-engineer personal information about individuals. Questions about trust and accountability have pushed the German government to adopt a decentralised model, after previously favouring a centralised model. The French parliament debated similar concerns, given that the French government plans to implement a centralised model.

The concerns raised by advocates and other stakeholders reflect the in-depth considerations that governments should undertake prior to implementing any contact tracing app, particularly when a large percentage of the population must download the app for it to be effective. Users will only download the app if they feel secure that their data is safe and protected.

How the mobile industry can help

MNOs will usually not be involved in implementing the app nor in any data. But there are still a number of aspects where MNOs could consider supporting:

- **Testing of apps**
  Interoperability on various devices and Bluetooth proximity measurement calibration. Some MNOs, e.g. Vodafone and Orange, are doing this already. In addition, the GSMA Terminal Steering Working Group is supporting work to gather device-specific Bluetooth calibration parameters from a broad reach of handset manufacturers and to provide this to all such initiatives to improve app performance

- **Increasing reach / dissemination of apps**

  - Integrate software into own apps (e.g. customer self-care app), if this is part of the national strategy
  - Pre-install on devices
  - Communicate to / educate subscribers

- **Zero-rating traffic of apps**
  Supporting user acceptance

- **Consulting parties implementing the apps**
  Consult on possible optimisation to, for example, mitigate the data volume challenge (e.g. foster WiFi offloading, ensure that the devices spread the communication across the whole day evenly)

- **Having a public policy opinion on data privacy**
  MNOs might be asked to provide an opinion on privacy even if no operator-controlled data is involved. There are many rumours, misunderstandings and concerns, and people are mixing-up different use-cases and solutions. MNOs can help to enter into a fact-based, transparent and reasonable discussion, and potentially more.

Appendix and further information

User experience and the Apple / Google Bluetooth proximity tracing capabilities

Implementing a proximity tracing application, which can only leverage the standard capabilities of a device's operating system to access the Bluetooth interface for proximity measurement, results in challenges regarding user experience and batter drain.

This has been reported for the early applications which have been developed in the UK and Australia:

- Critical mass of android users needed for success – The Guardian
- COVID-19 app not working on iPhones – The Guardian

Apple and Google have teamed-up to provide an enhanced capability, which can be integrated by proximity tracing apps to address a number of these topics. This joint initiative provides access to this capability of proximity tracing apps using the decentralised approach, which ensures, by technology, the highest level of data privacy.

How well can proximity be derived from Bluetooth signal strength?

A very detailed description of how proximity can be measured between two devices using Bluetooth Low Energy is given in a paper of the PEPP-PT initiative (co-operation across universities, research agencies and some companies in Germany, Austria, Switzerland, Netherlands, etc.). This paper explains how transmitter- and receiver-related calibration factors can be applied to account for technical differences between devices (chipset, antenna, chassis).

A related paper documents tests which validate how precise proximity can actually be measured by this methodology: github PEPP-PT.

How can an infection risk score be computed from the parameters (distance, duration) of a proximity event?

How to calculate an infection risk-score for a person who remained within a certain distance of an infected person for a certain period of time is explained in a paper of the PEPP-PT consortium. This paper explains the often found threshold values of 2 metres and 15 minutes.

A similar paper explains the definition of the risk score used in the UK proximity tracing app.

Overview of approaches and applications

Quite a comprehensive overview of the different approaches and app/solutions used in various countries can be found on Wikipedia.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com