BRIEFING

ITRE in Focus

European Parliament

National COVID-19 contact tracing apps

KEY FINDINGS

While the coordination of cross-border interoperable COVID-19 contact tracing apps is a competence of the European Commission, their development is a national competence. This short briefing summarises the current efforts towards, functionalities of and technical decisions on the development of national COVID-19 apps, with a focus on the ongoing centralised vs. decentralised approach and the interoperability of different apps across Europe. All Member States and the Commission consider the interoperability of the apps and backend servers to be essential for the effective tracing of cross-border infection chains, especially for cross-border workers and neighbouring countries. Ultimately, this effort will support the gradual lifting of border controls within the EU and the restoration of the single market's integrity.

Contact tracing apps

Several Member States in the European Economic Area (EEA) are currently implementing their COVID-19 contact tracing apps, with the aim of making them available to the general public in June 2020. Almost all contact tracing apps use a Bluetooth low energy (BLE) connection to automatically detect and trace all users' COVID-19 contacts, estimating their proximity on the basis of signal intensity. Each contact's risk of infection is calculated on both the phone of the infected individual and the phone of the contact using epidemiological thresholds of time and distance[1] maintained between the devices. If the measured exposure is epidemiologically relevant, the contact is recorded in the encrypted proximity history on both phones and deleted when it becomes epidemiologically unimportant. After receiving a positive COVID-19 test result from a public health authority, each user can consent to notify the app or a server[2] and transmit all relevant contact data to a server. Each exposed contact will then receive a warning message with specific information and guidance.

Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies

Authors: Matteo Ciucci, Frédéric Gouardères

PE 652.711 – May 2020

EN

Privacy-preserving apps

In this context, it is worth mentioning that contact data mainly refers to the arbitrary, encrypted and ephemeral COVID-19 identifiers of phones that have been in proximity to an infected user, and the contact's risk of infection data. The personal data attributes (name, phone number, etc.) and metadata (time of contact, signal intensity, other ancillary data, etc.) of all COVID-19 user identifiers are anonymised or pseudo-anonymised, in line with the General Data Protection Regulation privacy and data minimisation principles. The proximity history remains encrypted on the user's phone and cannot be viewed or transmitted by anybody. At any point in time, only the epidemiologically relevant proximity history is saved, and earlier history is continuously deleted. The explicit consent of the user is always required to allow the collection of any information that is not necessary for contact tracing, as well as to allow sharing with third parties. In almost all implementations of COVID-19 apps in the EU, no geo-positional data is collected due to data minimisation and privacy implications. A different approach has been taken by Norway, which plans to use GPS information for infection pattern tracking analysis. A radically different approach has been taken by China, which uses GPS data to assign QR code risk scores with three colours to determine the freedom of movement of each user.

Decentralised vs. centralised apps

COVID-19 apps split into two large groups according to their communication protocols. These groups mainly differ in storage location and/or the way they process COVID-19 arbitrary identifiers and contact data. Contact tracing apps can be distinguished between:

1) **Decentralised apps**: the arbitrary ephemeral identifiers of all phones in contact with another user are generated, stored and processed on the user's device (i.e. mobile phone), which calculates the risk scores for all users and stores all identifiers at risk of infection. When a person receives a positive COVID-19 test result from a public health authority, they upload their exposed contact data to a backend server. Examples of such systems include the DP-3T and TCN protocols and the Google-Apple Exposure Notification application programming interface (API).

2) **Centralised apps:** arbitrary ephemeral identifiers of all phones in proximity to the user are generated, stored and processed on a central server operated by the public health authorities, which calculates updated risk scores for all relevant users and decides which affected users to inform.

When a person receives a positive COVID-19 test result from a public health authority, they upload their exposed contact data to a backend server. Examples of such systems include ROBERT, PEPP-PT, and OpenTrace/BlueTrace/TraceTogether.

The distinction between the two groups is becoming more and more blurred. The difference between the centralised and decentralised protocols is not the existence of a backend server, as both the centralised and decentralised protocol implementations have one. The difference is actually the location of execution of certain key functionalities, such as the generation of unique identifiers and the calculation of epidemiologically effective risk scores based on contact risk data.

Contact data centralisation, which is built into the centralised approach, can be replicated in the decentralised protocol by voluntarily transmitting the contact data to a backend server after it has been collected. On the other end, the decentralised protocol relies on servers to store and process certain voluntarily shared contact tracing information. The recent statement of the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) organisation, which appears on its main webpage, makes the distinction between the two approaches even more blurred: 'PEPP-PT currently considers two privacy-preserving approaches: "centralized" and "decentralized", and continues to be open for further ideas for improvement that support PEPP-PT goals'.

The major concerns raised about the centralised vs. decentralised communication protocols therefore appear to relate to a mix of **security** and **privacy concerns, technical limitations** and **the market positions** of Google and Apple, the main smartphone operating system market players[3]. The initial implementation of the BLE function on Apple[4] showed that mobile phones did not seem to allow centralised apps running in the background to obtain and upload the history of all observed contacts. To perform such a function, the pre-13.5 version[5] of Apple's operating system would require either unlocked mobile devices to run the COVID-19 app in foreground, or would require the use of the BLE mode to be avoided, with a severe impact on battery duration. As a result of these technical limitations, some Member States and centralised protocol organisations (PEPP-PT) recently switched from a centralised to a decentralised approach (for information on the public debate, see the following reference pages: AT, DE, IE, IT).

The Apple-Google contact tracing partnership

On 10 April 2020, Google and Apple announced a two-phase exposure notification solution that uses Bluetooth technology on mobile devices to assist with contact tracing efforts. In the first phase planned for May 2020, both companies will release APIs that allow the contact tracing apps of public health authorities to work across Android and iOS devices, while maintaining user privacy. Once the app is launched, the user will need to consent to the terms and conditions before the program becomes active. In the second phase, available in the coming months, this capability will be introduced at the operating system level to help ensure broad adoption. After a consent-based operating system update, the system will send out and listen for the Bluetooth beacons as in the first phase, but without requiring an app to be installed. On 20 May 2020, the exposure notification APIs were first made available on iOS as part of the iOS 13.5 update.

Interoperability at EU level

The major issue with having many different national COVID-19 contact tracing apps is not knowing whether they will function when citizens of one country travel to another. Having to use multiple apps when travelling could further complicate an unproven technology and would mean trying to repurpose standard smartphone components to estimate viral exposure, a task for which mobile devices were never intended. The interoperability of contact tracing apps among Member States and apps is therefore key: all social tracing apps should be able to exchange the minimum amount of information necessary to alert individual app users, wherever they are located in the EU, of an epidemiologically relevant exposure to a user who has COVID-19.

On 13 May 2020, the voluntary e-Health Network[6], which provides a platform for Member State authorities dealing with digital health, proposed guidelines for the cross-border interoperability of approved contact tracing mobile apps and associated procedures. Some open questions remain, over, for instance, the interoperability of centralised and decentralised contact tracing systems, the identification of good practices and mechanisms for information exchange on the functioning of apps, various privacy concerns, and data sharing with relevant public health bodies and research institutions, including the sharing of aggregated data with the European Centre for Disease Prevention and Control. The Member State authorities represented in the e-Health Network should establish a process of information exchange ensuring the interoperability of applications when cross-border scenarios are expected.

Whatever the approach taken by Member States with approved apps, all Member States and the Commission consider the interoperability of apps and backend servers to be essential for the effective tracing of cross-border infection chains, especially for cross-border workers and neighbouring countries. Ultimately, this effort will support the gradual lifting of border controls within the EU and the restoration of the freedom of movement and of the integrity of the single market. However, the success of the apps will also depend on an array of other parameters such as the general adhesion of the public to such systems, the critical mass of users and the technical stability and reliability of Bluetooth signals.

Main positions on centralised and decentralised approaches

Commission recommendation of 8 April 2020

(23) A common Union approach to the COVID-19 crisis has also become necessary since measures taken in certain countries, such as the geolocation-based tracking of individuals, the use of technology to rate an individual's level of health risk and ***the centralisation of sensitive data****, raise questions from the viewpoint of several fundamental rights and freedoms guaranteed in the EU legal order, including the right to privacy and the right to the protection of personal data […]*

(25) In accordance with the principle of data minimization, public health authorities and research institutions should process personal data only where adequate, relevant and limited to what is necessary, and ***should*** *apply appropriate safeguards such as pseudonymisation, aggregation, encryption and* ***decentralization****.*

Source: European Commission recommendation of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.

Commission guidance of 16 April 2020

(3.5) [...] Contact tracing and warning functionality – Data of the infected person

The apps generate pseudo-randomly ephemeral and periodically changing identifiers of the phones that are in contact with the user. One option is that the identifiers are stored on the device of the user (so called decentralised processing). Another option can provide that these arbitrary identifiers are stored on the server to which the health authorities have access (so called backend server solution). ***The decentralised solution is more in line***

with the minimisation principle. *Health authorities should have access only to proximity data from the device of an infected person so that they are able to contact people at risk of infection [...]*

Source: European Commission guidance of 16 April 2020 on apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01).

European Parliament resolution of 17 April 2020

(52) Takes note of the emergence of contact-tracing applications on mobile devices in order to warn people if they were close to an infected person, and the Commission's recommendation to develop a common EU approach for the use of such applications; points out that any use of applications developed by national and EU authorities may not be obligatory and that the generated data are not to be stored in centralised databases, which are prone to potential risk of abuse and loss of trust and may endanger uptake throughout the Union; ***demands that all storage of data be decentralised,*** *full transparency be given on (non-EU) commercial interests of developers of these applications, and that clear projections be demonstrated as regards how the use of contact tracing apps by a part of the population, in combination with specific other measures, will lead to a significantly lower number of infected people; demands that the Commission and Member States are fully transparent on the functioning of contact-tracing apps, so that people can verify both the underlying protocol for security and privacy, and check the code itself to see whether the application functions as the authorities are claiming; recommends that sunset clauses are set and the principles of data protection by design and data minimisation are fully observed.*

Source: European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (P9_TA(2020)0054).

European Data Protection Supervisor guidelines of 21 April 2020

(42) Implementations for contact tracing can follow a centralized or a decentralized approach (note: in general, the decentralised solution is more in line with the minimisation principle). ***Both should be considered viable options,*** *provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages. Thus, the conceptual phase of app development should always include thorough consideration of both concepts carefully weighing up the respective effects on data protection /privacy and the possible impacts on individuals rights.*

Source: European Data Protection Supervisor, guidelines of 21 April 2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

General Data Protection Regulation

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest, which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. ***Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread*** *or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.*

Source: Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (OJ L 119, 4.5.2016, p.1).

For more details on all of the above, see the Commission's guidance on apps supporting the fight against COVID-19 pandemic in relation to data protection, the eHealth Network's common toolbox for Member States on mobile applications to support contact tracing in the EU's fight against COVID-19 and its interoperability guidelines for approved contact tracing mobile applications in the EU.

Contact tracing apps as digital health solutions

Digital health solutions are a broad range of public, private and community-based initiatives to develop COVID-19 digital tools providing certain key functionalities that go beyond contact tracing, including:

- Contact tracing (Bluetooth-based) and tracking (GPS-based);
- Symptom checks and self-diagnosis;
- Trustworthy information for the public;
- Self-managed support for homebound diagnosed patients;
- Support from medical staff, mainly in the form of follow-ups on homebound patients.

The Inventory Mobile Solutions against COVID-19 gives a non-exhaustive overview of EU and worldwide digital solutions, in particular mHealth initiatives and digital apps, used in the response to the COVID-19 pandemic. In addition, several projects supported by Horizon 2020 provide e-catalogues of COVID-19 technologies already available on the market, such as the European mHealth hub, the eHealth Hub platform and the Active Assisted Living Programme (AAL Programme – Solutions Supporting Older Adults during the Coronavirus Outbreak). For more information, see the OECD Observatory of Public Health Information's COVID-19 Innovative Response Tracker.

National Contact Tracing Apps

The table provides an overview of official COVID-19 contact tracing apps:

Country	Function	Description and status
AT	Contact tracing + health functionalities	• Name: Stopp Corona • Operational • Voluntary • Decentralised • Github documentation • Bluetooth, based on the Google-Apple API
BE	-	• Under debate: the implementation of contact tracing applications is not envisaged in the near future and contact research should be performed manually. See also the recent declaration of the Belgian Data Protection Authority on contact tracing apps
BG	(Contact tracing) + virus monitoring	• Under consideration (the VirusSafe application provides virus monitoring, supporting very limited, real-time contact tracing functionalities)
CN	Contact tracing + symptoms checking + quarantine +	• Name: Health Code System • Operational • Obligatory • Centralised • Location-based

	Infection pattern tracking	• Use: each user receives a traffic-light QR code based on the user's contact history and showing their health status; it is necessary to display the code in order to access all private and public spaces open to public (see example)
CY	Contact tracing	• Name: CovTracer • Operational • Voluntary • Bluetooth + limited GPS, based on MIT SafePaths • Decentralised
CZ	Contact tracing	• Name: eRouška • Operational • Voluntary • Developed by the local IT community, released as open source • Bluetooth • Centralised
DE	Contact tracing	• Under development • Voluntary • Decentralised • Bluetooth
DK	Contact tracing + health functionalities	• Name: Smittestop • Under development • Voluntary • Bluetooth • Centralised
EE	Contact tracing	• Under development • Voluntary • Decentralised (DP-3T protocol) • Bluetooth
EL	Contact tracing	• Under development
ES	Contact tracing + health functionalities	• Under development • Voluntary • Bluetooth
FI	Contact tracing	• Under development • Voluntary • Decentralised
FR	Contact tracing	• Name: StopCovid • Operational • Voluntary • Centralised (ROBERT protocol) • Bluetooth • Partial GitLab documentation (see INRIA's statement)
HR	Contact tracing	• Under development

HU	Contact tracing	• Name: VirusRadar • Operational • Voluntary • Decentralised • Bluetooth
IE	Contact tracing + symptom checking + infection pattern (heat maps) visualisation and modelling	• Under development • Voluntary • Decentralised • Heat maps and modelling of the spread of the disease
IT	Contact tracing	• Name: Immuni • Operational • Voluntary • Decentralised • Bluetooth-based on Google-Apple • Open source
IS	Contact tracing	• Name: Rakning C-19 • Operational • Location-based • Github documentation
LT	Contact tracing + health functionalities	• Under development • Voluntary • Centralised
LU	Contact tracing	• Under development
LV	Contact tracing + health functionalities	• Name: Apturi Covid (Stop Covid) • Operational • Voluntary • Decentralised • Bluetooth-based on Google-Apple
MT	Contact tracing	• Under development
NL	Contact tracing	• Under development • Voluntary • Decentralised
NO	Contact tracing + infection pattern tracking	• Name: Smittestop • Operational • Bluetooth- and GPS -based • Under the patronage of the Norwegian Institute of Public Health • 30-days automatic data deletion or user-defined

PL	Contact tracing + self-diagnosis + [optional] quarantine support	• Name: ProteGO Safe • Under the patronage of the Ministry of Digitalisation • Bluetooth • Voluntary • Decentralised
PT	Contact tracing	• Name: MonitorCovid19.pt • Under the patronage of the Ministry of Health • Bluetooth • Voluntary • Decentralised
RO	Contact tracing	• Under development
SE	Contact tracing	• Under debate
SI	Contact tracing	• Under development
SK	Contact tracing + infection pattern tracking	• Name: Zostaň Zdravý • Operational • Voluntary • Bluetooth- and GPS -based • Centralised
UK	Contact tracing	• Name: NHS COVID-19 app • Under development • Voluntary • Centralised • Bluetooth-based

Source: eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States, Version 1.0, pp. 10-12 and Inventory Mobile Solutions Against COVID-19. European Union Agency for Fundamental Rights report Coronavirus Pandemic in the EU – Fundamental Rights Implications: With a Focus on Contact-Tracing Apps.

[1] Current epidemiological models assume that a distance of less than two metres over a period of at least 15 minutes puts individuals at an increased risk of infection.

[2] Under the centralised approach, it is not clear if the public health authority or the user themself is responsible for communicating the positive COVID-19 test result after each user's consent has been obtained.

[3] According to the International Data Corporation (IDC), the worldwide smartphone operating system market is split between just two providers: Android has 86.6 % and iOS has 13.4 %.

[4] This technical limitation does not seem to exist on Google's Android operating system.

[5] This statement applies to all iOS versions preceding version 13.4; iOS version 13.5 was released on 20 May 2020.

[6] The eHealth network was set up by the European Commission under article 14 of Directive 2011/24/EU.

IP/A/ITRE/2020-09; Manuscript completed: May 2020; Date of publication: May, 2020
Administrator responsible: Matteo CIUCCI; Editorial assistant: Catherine NAAS
Contact: Poldep-Economy-Science@ep.europa.eu
This document is available on the internet at: www.europarl.europa.eu/supporting-analyses

Print ISBN 978-92-846-6754-3 | doi: 10.2861/898168 | QA-02-20-396-EN-C
PDF ISBN 978-92-846-6755-0 | doi:10.2861/ 808426 | QA-02-20-396-EN-N