**OECD**

**TACKLING CORONAVIRUS (COVID-19)**
CONTRIBUTING TO A GLOBAL EFFORT

# Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics

## Key messages

- Digital technologies, in particular mobile and biometric applications, are being adopted in innovative ways to improve the effectiveness of government front-line responses to COVID-19.
- The resulting information and trends are invaluable for governments seeking to track the COVID-19 outbreak, warn vulnerable communities, and understand the impact of policies such as social distancing and confinement.
- Disclosures of personal information can allow the public to better identify potential COVID-19 infections and track the spread over time. However, current digital solutions for monitoring and containment have varying implications for privacy and data protection.
- Fully transparent and accountable privacy-preserving solutions should be embedded by design to balance the benefits and the risks associated with personal data collection, process and sharing. Data should be retained only for so long as is necessary to serve the specific purpose for which it was collected.

## Governments are collaborating with telecommunication service providers to access geolocation data to track population movements

As COVID-19 continues to take human lives and jolt the global economy, governments are urgently seeking innovative new tools to inform policy and tackle the crisis. Digital solutions based on geolocation

data are emerging to help authorities monitor and contain the spread of the virus. Some are fed by mobile call data records (CDRs), i.e. data produced by telecommunication service providers on telephone calls or other telecommunications transactions, which provide valuable insights into population movements. As network operators serve substantial portions of the population across entire nations, the movements of millions of people at fine spatial and temporal scales can be measured in near real-time. The resulting information and trends are invaluable for governments seeking to track the COVID-19 outbreak, warn vulnerable communities, and understand the impact of policies such as social distancing and confinement.

Telecommunications providers in a number of OECD countries have started to share CDR-based geolocation data with governments in an aggregated, anonymised format. For example:

- The German telecommunications provider Deutsche Telekom is providing anonymised "movement flows" data of its users to the Robert-Koch Institute, a research institute and government agency responsible for disease control and prevention.

- Vodafone Group's Five Point Plan to address COVID-19 includes providing governments with large anonymised data sets (such as an aggregated and anonymous heat map for the Lombardy region) to help authorities better understand population movements.

- The European Commission is currently liaising with eight European telecommunications operators to obtain from them anonymised aggregate mobile geolocation data, in order to coordinate measures tracking the spread of COVID-19. To address privacy concerns, the data will be deleted once the crisis is over.

## New mobile applications for COVID-19 "tracking" are also being launched

Mobile health advice apps already constitute an important part of the mobile health ecosystem and have proven effective for the purpose of prevention, early diagnosis (e.g. symptom checkers) and for connecting users to local health services and emergency units. Now, new consumer-facing applications are emerging aimed at COVID-19 tracking. These applications are increasingly developed as open source and are the product of partnerships of tech companies, academia, clinicians and public authorities, which are ultimately responsible for their funding, further development and implementation. While not necessarily capturing all the population (e.g. the elderly who may not have, or be proficient in the use of, smartphones), nor without some error (e.g. when unable to distinguish between people in the same household and those in surrounding residences), these apps provide another tool for governments to monitor and contain the virus. Among the most cited are:

- **TraceTogether**: Developed by the Government Technology Agency of Singapore (GovTech) in collaboration with the Ministry of Health, using Bluetooth, this app tracks individuals who have been exposed to the virus. This information is used to identify close contacts based on the proximity and duration of an encounter between two users. It then alerts those who come in contact with someone who has tested positive or is at high risk for carrying the coronavirus. Once an individual is confirmed or suspected to be infected, they can choose to allow hospitals, the Ministry of Health and third parties to access data in the app to help identify close contacts. Singapore is planning to make the underlying privacy-preserving protocol for data exchange that TraceTogether is based on open source.

- **Pan-European Privacy-Preserving Proximity Tracing**: Over 130 scientists, technologists and experts from eight European countries – including France, Germany and Italy – took part in a non-profit initiative that developed an open source app which analyses Bluetooth signals between mobile phones to detect users who have been in close proximity to each other. The app temporarily stores that encrypted data locally, and if the users later test positive for COVID-19, it can alert anyone who has been around the infected individual in the preceding days, while keeping all users' identities protected.

- **Korea's Tracking App**: Funded by the Korean government this GPS-based tracking app is used by public authorities to locate possible sources of COVID-19 infection for further investigation and warn

citizens. The app can also be used for self-checking and voluntarily reporting. It can help officials identify hot beds of infection and has been used as an aid to track and control the pandemic.

- **C-19 COVID Symptom Tracker**: The aim of this app developed in the United Kingdom as a partnership between doctors and scientists at King's College London, a health data science company (a spin-out from King's), and the National Institute of Health Research Centre at Guy's and St Thomas' Hospitals is to slow the outbreak of COVID-19 by helping researchers identify: i) how fast the virus is spreading in different areas; ii) high-risk areas in the United Kingdom; and iii) who is most at risk, by better understanding symptoms linked to underlying health conditions. According to researchers, the data from the study can reveal essential information about the symptoms and progress of infection in different people. It can also help researchers understand why some individuals go on to develop more severe or fatal symptoms while others have only mild symptoms due to COVID-19.

- In addition, **Apple and Google** will also release APIs that enable interoperability between Android and iOS devices using apps from public health authorities. Users will be able to download these apps via their respective app stores. The two companies will also work together to enable a broader Bluetooth-based contact tracing platform by building this functionality into the underlying platforms. This solution would allow more individuals to participate in case they decide to opt in and could enhance interaction with a broader ecosystem of apps and government health authorities.

## Tracking apps can embody varying degrees of privacy and data protection

The use of geolocation data-collecting apps can allow data-sharing with explicit, built-in privacy and data protections, and enable users to give their explicit, informed consent to the collection and sharing of their personal data (assuming use of the app is not mandatory). For instance, Singapore's TraceTogether app has a number of privacy safeguards, including that it does not collect or use geolocation data and data logs are stored in an encrypted form. To protect the privacy of its users, the Pan-European app encrypts data and anonymises personal information. In addition, as two phones never exchange data directly and the users' aliases are changed frequently, it is virtually impossible to reveal the identity of users.

However, the range of personal data these apps collect, process and share can be very broad and difficult for users to understand. In many cases, apps continue to run in the background even when the device is not in use. Some apps can also exchange information with other apps through application programming interfaces (APIs), generating more detailed information. While the World Health Organization (WHO) praised Korea's extensive tracing measures, the sharing of location data collected by the GPS tracking app has raised privacy concerns. In response, the Korean government published recently a revised guideline for its used based on the Infectious Disease Control and Prevention Act passed in 2010 which does not allow any information specific to the data subject to be disclosed.

## Leveraging biometric data adds both benefits and challenges

Facial recognition has been one of the most frequently used biometrics in a number of countries to monitor the spread of COVID-19. Facial recognition enables authorities to reduce the use of identification technologies that require physical contact (such as iris scans and fingerprints). It can also be paired with other technologies, including thermal imaging enhanced by artificial intelligence, to better track citizens who may test positive for COVID-19.

In Poland, the government has launched a biometrics smartphone app to confirm that people who are infected with COVID-19 remain under quarantine. In the People's Republic of China (hereafter "China"), facial recognition has been used to prevent citizens who may be infected with COVID-19 from travelling. In addition, companies in China have developed a technology that could allow the government to successfully

identify people even when they are wearing masks. In the Russian Federation, facial recognition systems are being used to track individuals who fail to respect mandatory quarantine.

However, the use of biometrics (including facial recognition) in response to COVID-19 raises a number of privacy and security concerns, particularly when these technologies are being used in the absence of specific guidance or fully informed and explicit consent. Individuals may also have problems exercising a wide range of fundamental rights, including the right of access to their personal data, the right to erasure, and the right to be informed as to the purposes of processing and who that data is shared with. Facial recognition systems can also have inherent technological bias, e.g. when based on race or ethnic origin.

## Privacy-by-design can help address the risks

Privacy-by-design seeks to deliver the maximum degree of privacy by ensuring that personal data protections are built into the system, by default. Privacy-by-design may, for example, involve the use of aggregated, anonymised, or pseudonymous data to provide added privacy protection, or the deletion of data once its purpose is served.

For instance, the COVID-19 app developed by the Norwegian Institute of Public Health is designed to store location data only for 30 days. The use of additional privacy enhancing solutions (such as homomorphic encryption)[1] may provide added security, as can the use of data sandboxes, through which access to highly sensitive (personal) data is only granted within a restricted digital and/or physical environment to trusted users. An example of the latter is Flowminder, which collaborated with telecommunication companies during the 2014-16 Ebola outbreak to provide epidemiologists with secured access to de-identified low-resolution geolocation data. Flowminder is using a similar strategy in contributing to the response to the COVID-19 crisis.

## Key recommendations

Digital technologies provide powerful tools for governments in their fight to control the COVID-19 pandemic, but their privacy and data protection implications must be recognised. Contact-tracing apps should be implemented with full transparency, in consultation with major stakeholders, robust privacy-by-design protections, and through open source projects (where appropriate). Governments should consider:

- The legal basis of the use of these technologies, which varies according to the type of data collected (e.g. personal, sensitive, pseudonymised, anonymised, aggregated, structured or unstructured).
- Whether the use of these technologies and the subsequent data gathering is proportionate, and consider how the data is stored, processed, shared and with whom (including what security and privacy-by-design protocols are implemented).
- The quality of the data collected and whether it is fit for purpose.
- Whether the public is well-informed and the approaches adopted are implemented with full transparency and accountability.
- The time period within which more invasive technologies that collect personal data may be used to combat the crisis. Data should be retained only for so long as is necessary to serve the specific purpose for which it was collected.

---

[1] Allows processing of encrypted data without revealing its embedded information.

## Further reading

OECD (2019a), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en.

OECD (2019b), *Recommendation of the Council on Artificial Intelligence*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

OECD (2017), *Recommendation of the Council on Health Data Governance*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433.

OECD (2015), "Mobile technology-based services for global health and wellness: Opportunities and challenges", webpage, OECD, Paris, www.oecd.org/sti/ieconomy/mobile-technology-based-services-for-global-health.htm.

OECD (2013), *Recommendation of the Council concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

The OECD is compiling data, information, analysis and recommendations regarding the health, economic, financial and societal challenges posed by the impact of coronavirus (COVID-19). Please visit our dedicated page for a full suite of coronavirus-related information.