Opinion

EMBO reports

Data protection during the coronavirus crisis

Christophe Olivier Schneble*, Bernice Simone Elger & David Martin Shaw

The SARS-CoV-2 virus has caused a worldwide pandemic with many deaths (WHO, 2020b) and healthcare systems being pushed to their limits. This makes it all the more important to identify infected people early on and to ensure that people comply with public health measures so as to reduce the spread of the virus. In contrast to most previous pandemics, we can now use smartphone and other digital data. This is not the first case of using smartphone data for public health: The WHO's go.data initiative successfully used those technologies to fight Ebola (WHO, 2020a). Common to all digital tracking methods is the fact that we deal with different types of data, such as geo-localization data or, via Bluetooth, close-contact data, that under normal circumstances would fall within the scope of data protection laws. However, there is growing evidence that governments that using such technologies in conjunction with other basic hygiene measures are more successful in fighting COVID-19 (Ferretti *et al*, 2020; Normile, 2020). The question remains of how data protection regimes should react to such states of emergency.

Many data protection regulations are based on individual liberty rights. Legislation such as the EU's General Data Protection Regulation (GDPR) safeguards the privacy rights of citizens, ensuring that data are only processed if there are reasonable grounds for doing so. The GDPR mentions public health in particular as such a reason, but the Regulation also ensures that any processing follows rigorous procedures to minimize privacy breaches. In times of pandemic, though, another key value is saving lives, which can be in tension with privacy rights and individual autonomy. Given that people have already sacrificed their physical liberty by staying at home, we must consider whether and to which extent their right to privacy may also have to be compromised to facilitate the public health response. As more measures are taken to restrict liberty in order to protect the population, it makes also sense that data protection should follow this shift and allow governments or researchers to use smartphone data.

One question raised is whether highly identifiable geo-localization data are needed to track people's movements or whether it is sufficient to use anonymized proximity data using Bluetooth to notify those who have been in contact with someone infected by the coronavirus. Another important consideration is to use only the minimum amount of data to achieve effective contact tracing.

Several countries have now launched tracing apps most of which only acquire proximity data (Table 1). The data are encrypted on the phone, and many apps require user consent to share the data. Google and Apple have been developing an API embedded in their operating systems that enable homogeneity between apps and countries that rely on the API and its privacy specifications (https://www.apple.com/covid19/contacttracing).

The EU parliament stressed that any digital measures against the pandemic must conform with current data protection and privacy legislation. Fundamental principles include the voluntary use of such apps and sunset clauses to stop usage of the app once the pandemic is over (European Commission, 2020). The legal basis for processing is in line with the GDPR if the user gives consent, which "should be 'freely given', 'specific', 'explicit' and 'informed' within the meaning of the GDPR. It should be expressed through a clear affirmative action of the individual; this excludes tacit forms of consent (e.g., silence; inactivity)" (European Commission, 2020).

In the USA, the CDC developed a guidance for case identification and contact tracing plans (US Department of Health and Human Service C of DC and P, 2020). However, legal regulation across the USA remains heterogenous, mainly owing to the fact that federal law in form of the HIPAA safeguards only applies to covered entities: healthcare providers, health plans, and healthcare clearinghouses. Various states such as New York, New Jersey, and California have therefore set up their own regulations.

Tracing apps offer benefits on multiple levels: If they help to avoid exponential spread, fewer people will die and the economy will be less affected, thus preventing job losses. The basic ethical issues remain the same and have been discussed extensively for many years (Mittelstadt & Floridi, 2016).

It is essential that as many people as possible use tracing apps and it is therefore questionable whether consent on an individual basis is the right mechanism. Some governments have claimed the right to compel people to install the app and see this as a lower degree of interference with individual rights than other forms of confinement that many governments have imposed.

It goes without saying that *confidentiality, privacy, and transparency* are important. Data should only be used for the defined purpose of preventing further spread of SARS-CoV-2. Transparency is key to acceptance and use of an app.

Data minimization is one of the fundamental principles of data protection. Most of

University of Basel, Institute for Biomedical Ethics, Basel, Switzerland
*Corresponding author. E-mail: christophe.schneble@unibas.ch
DOI 10.15252/embr.202051362 | EMBO Reports (2020) 21: e51362 | Published online 11 August 2020

Table 1. Overview of selected contact tracing apps (Howell *et al*, 2020).

App (Country)	Developer	Data collected	Data sharing	Google/Apple APi
TraceTogether (Singapore)	Government Agency of Singapore/ Ministry of Health	Proximity Data (Bluetooth)	Only possible once exposed to a case. Sharing data to find others	No
Pan-European Privacy-Preserving Proximity Tracing	Scientists/Non-profit Initiative	Proximity Data (Bluetooth)	Alerts anyone that has been within s range	No.
Tracking App (Korea)	Korea Government	Health Monitor Data provided by the patient	With Government (Self-health status assessment)	No
Corona-Warn-App (Germany)	Robert Koch Institute	Proximity Data (Bluetooth)	Alerts others in contact with positive Tested Person upon consent	Yes
Swiss Covid (Switzerland)	Federal Office of Public Health FOPH	Proximity Data (Bluetooth)	Alerts others in contact with positive Tested Person upon consent	Yes
Stop Covid (France)	Gouvernement Francais	Proximity Data (Bluetooth)	Alerts others in contact with positive Tested Person upon consent	No
COCOA (Japan)	Ministry of Health and Labour and Welfare	Proximity Data (Bluetooth)	Alerts others in contact with positive Tested Person upon consent	Yes

the current apps adhere to this principle by collecting only the random key broadcasted by the API. However, public authorities might want to access location data to monitor and reconstruct movement patterns. This could help to prevent a lockdown of smaller areas as it happened recently in Germany after infection of meatpackers in a slaughterhouse.

Strongly intertwined with *consent* to process individual data is *data sharing*. Fighting COVID-19 relies on detecting cases and informing others about potential exposure. This results in an ethical dilemma: From a public health perspective, it would be beneficial to automatically share a positive result, but this would require identifying individuals. Balancing the risk of spreading the virus, it remains questionable why exposed persons and the authorities are not automatically notified especially as some disease prevention laws enable mandatory quarantine.

Although many people see the use of cell phone data as the first steps on a slippery slope toward surveillance of citizens, it can be argued that the use of these data and the abandonment of informational self-determination are justified in view of the public good. However, data use and access must remain proportional to the degree of the emergency and threat of loss of lives. Thus, the use of such data should only be allowed under certain conditions delineated in the following.

First, the government should limit the timeframe during which data can be used for monitoring or contact tracing *(sunset clause)*. Using such an invasive tracing of large groups must remain an exception and should not be used to pursue a political agenda. Therefore, a periodic reevaluation is required to guarantee the sole use of data for the specific purpose of monitoring infections.

Second, using identifiable cell phone data for monitoring without consent should be limited to governments under the aforementioned premises, and any such use must be justified and proportional: The benefits resulting from tracking individuals must be significantly greater for society than the potential loss of privacy. In addition, any such use of data must not contravene any national laws.

Third, apps need to implement state-of-the-art consent mechanisms or have to be democratically endorsed before implementation. Uptake and efficiency will highly depend on transparency and user confidence. Transparency is a key for success; without it, app penetration will not reach sufficient numbers to defeat the virus. Decentralized data excluding geo-localization should be used as long as this permits efficient contact tracing and people comply with quarantine measures on their own (Thüsing *et al*, 2020). Lastly, apps should be justified by strong scientific arguments. If any of these conditions are not fulfilled, use of the app should be terminated. Ethical digital contact tracing is possible, but certain standards must be met.

References

European Commission. Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection. 2020 Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29

Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Bonsall DG, Fraser C (2020) *medRxiv*

Howell O'Neill P, Ryan-Mosley T, Johnson B. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. MIT Technology Review. 2020 Available from: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

Mittelstadt BD, Floridi L (2016) *Sci Eng Ethics* 22: 303 – 341

Normile D (2020) Coronavirus cases have dropped sharply in South Korea. What's the secret to its success? *Science*. https://www.sciencemag.org/news/2020/03/coronavirus-cases-have-dropped-sharply-south-korea-whats-secret-its-success

Thüsing G, Kugelmann D, Schwartmann R (2020) *Datenschutz-Experten beurteilen Corona-App*. Frankfurt: Frankfurter Allgemeine

US Department of Health and Human Service C of DC and P. Interim Guidance on Developing a COVID-19 Case Investigation & Contact Tracing Plan [Internet]. 2020. Available from: https://www.cdc.gov/coronavirus/2019-ncov/downloads/case-investigation-contact-tracing.pdf

WHO (2020a) Go.Data: Managing complex data in outbreaks [Internet]. Available from: https://www.who.int/godata

WHO (2020b) WHO Director-General's opening remarks at the media briefing on COVID-19 [Internet]. [cited 2020 Apr 1]. Available from: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020

