

The protection of privacy and personal information. How much personal information will be enough?

24 April 2020 6 min read

One Covid-19. So many tracing apps to locate individuals.

"Your recently announced project to respond to COVID-19 by tracking when and where Americans interact with each other raises serious concerns... I fear that your project could pave the way for something much more dire." United States Senator Josh Hawley

Since the inception of the COVID-19 pandemic, Governments and health authorities across the world have been working to find solutions to combat the COVID-19 pandemic. Technology giants Google and Apple have now joined this fight with its announcement of a contact tracing technology to help Governments and health authorities reduce the spread of COVID-19, stating that user privacy and security are central to the design.^[1] This contact tracing system will use randomised ID's not tied to a user's actual identity information to communicate potential contacts with individuals with a confirmed positive COVID-19 diagnosis. Apple and Google announced that this system is decentralised and never collects any geography data in order to preserve individual privacy.

The question is, what will history show in years to come.

On 25 March 2020, the Minister of Communications, Telecommunications and Postal Services, Stella Ndabeni-Abrahams ("**the Minister**") announced that cell phone data will be utilised in South Africa to curb the spread of the novel COVID-19.^[2] In this regard, chapter 3 of the Regulations issued in terms of section 27(2) of the Disaster Management Act 57 of 2002 ("**the Regulations**") provides for the establishment of a Covid-19 Tracing Database ("**Database**"). The National Department of Health ("**the Department**") is responsible for the establishment of this Database. Furthermore, in terms of Regulation 11H(2), the Department is mandated to –

"develop and maintain a national database to enable the tracing of persons who are known or reasonably suspected to have come into contact with any person known or reasonably suspected to have contracted Covid-19" [Emphasis added]

Looking further abroad, the European Data Protection Board has repeatedly stated that the implementation of data protection principles and respect of fundamental rights and freedoms is not only a legal obligation, but also a requirement to be reinforced when considering and implementing any data-based initiatives for combating the spread of the COVID-19 virus and for informing de-escalation strategies.

History has shown that in times of major crises, governments and other organisations, endeavour to put in place mechanisms to assist in collating sufficient information in order to interpret any threat to the general population. But, if not managed responsibly, such initiatives could have significant unintended consequences.

The World Health Organization ("**WHO**") has issued interim guidance on Global surveillance for COVID-19. In terms of the WHO guidance, public health surveillance can be defined as the continuous, systematic collection, analysis and interpretation of health-related data needed for the planning, implementation, and evaluation of public health practice in relation to COVID-19.

Recognising the importance of public health, one should also remember that it is a very sensitive balancing act to protect individual privacy, a fundamental human right, on the one hand and the collection of health information of individuals, that is critical to the public good and public health, on the other. The ability to identify hot-spot areas where infections are prevalent, is without doubt crucial.

In a time where urgent and speedy innovation is required, where companies and researchers operating without the luxury of time, a danger exists that guidelines could be seen as a hindrance, preventing innovation. [Kay Firth-Butterfield](#), the World Economic Forums leader of the Centre for the Fourth Industrial Revolution and of artificial intelligence and machine learning recently stated that:

“We need to keep in mind that the big ethical challenges around privacy, accountability, bias, and transparency of artificial intelligence remain”

The European Data Protection Board has warned that invasive measures, such as the “tracking” of individuals could be considered proportional under exceptional circumstances. However, this must go hand in hand with the implantation of safeguards to ensure data protection principles are not disregarded.

Safeguards that both Government as well as developers and innovators must implement, must link directly to the extent and duration of COVID-19. Any authorisation for the acceptance and implementation of surveillance tools must carry with it the responsibility to ensure that the necessary checks and balances are present to prevent miss-use and that remedies to rectify abuse of processes and information are sound. The right to privacy cannot be completely ignored because of COVID-19.

The European Data Protection Board has adopted that in principle, location data can only be used when made anonymous or with the consent of individuals. The aim of Contact tracing apps should not be to follow the movements of individuals. The main function of such tracing apps should be to identify events where COVID-19 positive individuals were present. The mere collection, through location tracking, of all movements by an individual, is contrary to the principle of data minimisation as provided for in privacy legislation.

In its guidance, the [Dutch Autoriteit Persoonsgegevens](#) referenced a study, that analysed the mobility data of 1.5 million individuals over a period of 15 months and found that four spatio-temporal points are enough to identify 95% of individuals. The authors of the study concluded that location data “provides little anonymity” and therefor statements and assurances that location data will be anonymised are of no value when seen through the lens of data privacy.

Overall envisaged location tracing apps should be developed in line with data protection principles, and allow for mechanisms to ensure that individual can exercise their rights and freedoms.

The core message at this point in time is that in times where speedy innovation is of great importance, considering privacy legislation, any innovation providing for the collection of personal information should ensure that collection is minimised and retention limited. Limiting access and retaining data only for the minimum amount of time it is needed for, can reduce the harms that may arise from secondary, unintended and potentially harmful uses of COVID-19 data.

Privacy is unequivocally recognised as a fundamental human right in terms of the South African Constitution. It should be respected, always and more so in time such as the present.

[1] D Etherington ‘First version of Apple and Google’s contact tracing API should be available to developers next week’ available at <https://techcrunch.com/2020/04/23/first-version-of-apple-and-googles-contact-tracing-api-should-be-available-to-developers-next-week/>, accessed on 24 April 2020.

[2] The Minister announced this at the Security Cluster Meeting held on 25 March 2020. Available at <https://youtu.be/aBzDYCWFFIM>, accessed on 24 April 2020.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)