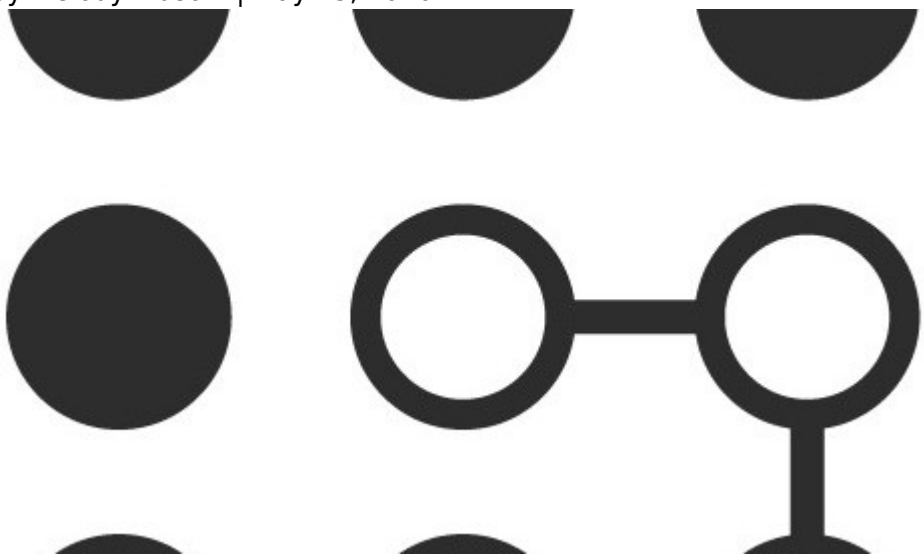
CONTACT TRACING MOBILE APPS: RECOMMENDATIONS FROM THE EUROPEAN DATA PROTECTION BOARD

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Melody Musoni | May 15, 2020



By now, everyone knows that certain constitutional rights can be limited in order to serve a public interest such as public health. However, concerns around privacy protection keep mounting, especially so with the implementation of lockdown regulations on contact tracing.[1] Contact tracing is being implemented on a global scale with countries leveraging different technologies to prevent the spread of COVID-19. China, the original epicentre of the virus, introduced mobile apps like 'Alipay Health Code App'[2] where users fill in their personal information and the app determines whether a person should be quarantined or allowed into public spaces. Norway also introduced its 'Smittestop App' which alerts users of the app if they have been in contact with someone with COVID-19.[3] Additionally, Singaporean government is urging its citizens to make use of 'TraceTogether App'.[4]

South Africa has not adopted any contact tracing mobile apps yet, but the lockdown regulations have empowered the Director General of Health to develop and maintain a database with information of persons who have been tested for COVID-19 as well as information of persons who have come in contact with those who tested positive for COVID-19. At the same time, the lockdown regulations permit the Director General to direct telecommunications service providers (like MTN, Vodacom, and Cell C) to provide information regarding the location or movements of COVID-19 patients or persons they may have come into contact with. The Information Regulator published its Guidance note[5] on the processing of personal information during the pandemic. The Information Regulator clarified that electronic service providers can provide mobile location-based data of persons and that government can use such personal information for purposes of conducting mass surveillance of data subjects if the personal information is anonymised or de-identified in a way that prevents its reconstruction in an intelligible form. The lockdown regulations seem not to address mobile application technologies which may be used for contact tracing.

In Europe, the European Data Protection Board (EDPB) has published its guidelines on the use of location data and contact tracing tools.[6] These EDPB guidelines provide comprehensive and detailed measures that need to be implemented by service providers who may wish to make use of mobile contract tracing apps. The EDPB guidelines can be exemplary for South Africa, particularly with regard

to contact tracing apps. For instance, the EDPB guidelines emphasise the importance of data minimisation, and that mobile applications should not collect unrelated or unnecessary information. This information may include civil status, communication identifiers, equipment directory messages, call logs, or location data and device identifiers. These recommendations are also in line with the Protection of Personal Information Act's (POPIA) condition on data minimality. POPIA provides that one must collect information that is relevant and adequate and avoid excessive collection of personal information.

The EDPB guidelines also recommend that implementation of contact tracing can follow a centralised or a decentralised approach. 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 individual rights. The EDPB guidelines also recommend the implementation of the use of state-of-the-art cryptographic techniques which secure data stored on servers and applications, and encrypts exchanges between applications and the remote server. At the same time, mutual authentication between the application and the server must also be performed.

The reporting of users who are infected with COVID-19 must be subject to proper authorisation, for example, through a single use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, no data processing that presumes the validity of the user's status should take place.

With Apple and Google working on coronavirus mobile tracing systems[7], it is a matter of time before South Africa implements mobile tracing apps to deal with COVID-19. It is therefore important that when the time comes, we consider adopting recommendations from the EDPB guidelines.

[1] Disaster Management Act, 2002: Amendment of Regulations issued in terms of section 27 (2) GG 43199 GN 446 of 2 April 2020.

[2] https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

[3] https://www.thestar.com.my/tech/tech-news/2020/04/17/covid-19-norway-launches-virus-tracker-app

[4] https://qz.com/1842200/singapore-wants-everyone-to-download-covid-19-contact-tracing-apps/

[5] Guidance Note on the Processing of Personal Information in the Management and Containment of COVID-19 Pandemic in terms of the Protection of Personal Information Act 4 of 2013.

[6] European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Adopted on 21 April 2020.

[7] https://www.reuters.com/article/us-apple-google-contact-tracing/apple-google-update-coronavirus-contact-tracing-tech-ahead-of-launch-idUSKCN2262NT.