WERKSMANS
ATTORNEYS

REGULATORY

As little as possible infringement? Is this the case when thinking about the right to privacy in South Africa?

8 May 2020 *7 min read*

by Ahmore Burger-Smidt, Director and Head of the Data Privacy practice

A year back there would have been a massive outcry if anyone contemplated for governments to track individuals via mobile phones, but the coronavirus pandemic has resulted in a slightly re-aligned debate. Techniques that were once seen as intrusive, like collecting location and health data, are now part and parcel of government plans to contain the virus.

But the tracking of individuals through mobile phone data or apps, means that the associate metadata potentially tells a very revealing story of what an individual does, where and when he/she does it, and with whom. And there goes privacy. Or potentially.

Chapter 2 of the Regulations issued in terms of section 27(2) of the Disaster Management Act, 2002 as published on 30 April 2020 ("**the Regulations**"), provides that any Cabinet Member may issue and vary directions, as required, within his or her mandate, to address, prevent and combat the spread of COVID-19, including the dissemination of information required for dealing with the national state of disaster.

Also, these Regulations provide specifically, for "Contact tracing" and a "COVID-19 Tracing Database" meaning a database established by the National Department of Health which the National Department of Health shall develop and maintain 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. But more importantly, the Director-General: Health may, in writing and without prior notice to the person concerned, direct an electronic communications services provider to hand over to the Health Department, for inclusion in the COVID-19 Tracing Database, information regarding:

- the location or movements of any person known or reasonably suspected to have contracted COVID-19; and
- the location or movements of any person known or reasonably suspected to have come into contact, during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated.

As citizens, every individual should have the assurance, not just statements of reassurance, that data collated will not be shared across various government without a clear rationale or requirement underlining the sharing, with law enforcement agencies, or hackers.

Unfortunately, in South Africa, we lack robust data protection legislation. Irrespective of regulations providing for criminal sanctions and penalties that were announced on 6 May 2020 (these are in any event negligible) we are left wondering whether a backdoor of vulnerability, enabling data leakage or misuse, or other use that is contrary to the interests of those individuals being traced, through the use of mobile tracking, exists.

Countries around the world are contemplating the roll-out of tracking methods to help the authorities contain its spread of COVOD-19. But as a global COVID-19 database begins to mushroom, privacy concerns are prevalent.

Apple and Google are focussing on the development of "Exposure Notification". The coronavirus tracing tool developed by Apple and Google, unveiled in April 2020 and to be launched during mid-May 2020, adds technology to the iOS and Android

smartphone operating systems that alerts users, notably anonymously, if they have come into contact with a person with Covid-19. In terms of the encryption specification that Apple and Google have added to "Exposure Notification", daily tracing keys will be randomly generated rather than mathematically derived from a user's private key. Crucially, the daily tracing key is shared with the central database if users decide to report their positive diagnosis.

In India is reported that the Indian government is pushing smartphone makers to preinstall its coronavirus tracker which was officially launched end of April 2020. It is a coronavirus contact tracing app named Aarogya Setu. It has already reached the milestone of 80 million downloads.

Further afield in Ghana, a software engineering company, Cognate Systems, is using technology to track coronavirus symptoms and hotspots in the West African country. Using a platform called Opine Health Assistant, the company is able to record and track the frequency of coronavirus symptoms like a cough and high temperature in different parts of the country. The platform collects information from individuals about their possible coronavirus symptoms and location through a USSD short code on their mobile phones. This is done on a voluntary basis by mobile users.

In Germany a model for a contact tracing app that protects personal data has been developed by an interdisciplinary team at the Technical University of Munich ("**TUM**"). The researchers have created an encryption process that enables people who have come into close contact with a COVID-19-positive individual to be warned without their phones recognising the infected person's temporary contact number ("**TCN**"). Mobiles on which these apps are installed use Bluetooth technology to exchange randomly generated TCNs, which constantly change. The TCNs are collected locally on the devices and stored for a limited period. If someone tests positive for COVID-19, that person's contacts are immediately notified. Through an encryption process called private set intersection cardinality, the TUM team have found a means of cross-checking TCNs of infected individuals against those collected on mobile phones without the need to load the TCNs onto their contact's phones. Kilian Holzapfel a physicist with TUM explain this outcome as follows:

"*As a result, the risk scenario in which an attacker could combine the received TCNs with other information such as the date, time and location where the TCN was transmitted – which would endanger the anonymity of an infected person – is minimized to a large extent*,"

But in South Africa, no consent is sought from an individual. Also, the decision to partake and voluntarily disclose our personal information, let alone the extend thereof, is not that of a citizen. As citizens we do not know what mechanism to delete data are in place or even considered. We do not know how personal information is being secured and how and if employees and vendors are being supervised. We do not even know if and where we can inquire or complain about our personal data being incorporated and held in terms of the COVID-19 Tracing Database.

It is important from a data protection perspective that the Department of Health's responsibilities should include managing the shared risk that other departments, to whom the Department of Health entrusts the COVID-19 Tracing Database information, to safely and securely manage that data.

The required levels of digital trust across a broad and diverse community, that the COVID-19 Tracing Database will only be used in the control and management of COVID-19, cannot be built only upon statements of good intent and Regulations not addressing security measures. Reassurance of good intent and legislated constraints are necessary, but insufficient steps to demonstrate safe and secure management of COVID-19 Tracing Database, cannot be a silent feature.

We know that the Protection of Personal Information Act, 2013, provides legal grounds to enable the employers and public health authorities to process personal data in the context of COVID-19, without the need to obtain the consent of individuals. We also know that contact tracing is seen as a crucial tool in slowing the spread of COVID-19 and helping to end lockdown measures.

Empowered, effective and real-time independent oversight and verification, and prompt and public reporting as to oversight and verification is an important factor in nurturing trust. We have not seen public reporting.

The concerns over individual privacy regarding the use of the personal information collected, security of information, including the extended time frame over which personal information will be collected (even though an individual could very well not be COVID-19 positive) and fears that the personal data collected could be targeted by cyber-criminals, cannot be ignored.

Food for thought?



Ahmore Burger-Smidt

Head of Regulatory

View Profile