SOUTH AFRICAN COVID-19 MOBILE TRACK AND TRACE LAWS – SHOULD WE BE WORRIED?

Category: Administrative and Procurement Law,Commercial Law,Dispute Resolution,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | April 1, 2020

In last night's update on the Covid-19 pandemic, South Africa's President Cyril Ramaphosa announced that "*Using mobile technology, an extensive tracing system will be rapidly deployed to trace those who have been in contact with confirmed coronavirus cases and to monitor the geographical location of new cases in real time.*"

You may ask: What about my right to privacy? What about the Protection of Personal Information Act (POPIA) and the protection it gives me? After all, my geographical location data is personal information that obliges others to protect it, so why is the State suddenly allowed to track my every move?

Well, POPIA does protect your personal information, which includes location data. Except, there are certain instances which are exempt from POPIA. Once of these instances is where a public body, such as the Department of Health or the South African Police Services, is involved in activities such as public safety.

This means that POPIA's protections, such as obtaining your consent, will not apply. All is not lost however. POPIA does say that, where it does not apply and therefore does not protect your personal information, your location data must be protected by another law.

But even if there is another law that protects the way in which location data is processed, it is still a very draconian approach, so why is it permitted. The reality is that because a pandemic like Covid-19 is such a serious threat, even countries that uphold the strongest democratic principles, believe that such measures are necessary. The European Union probably has the most stringent data protection laws in the world. Its European Data Protection Board (EDPB) said the following regarding using technology to fight Covid-19:

"*It is in the interest of humanity to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world. …Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data and in all cases it should be recalled that any measure taken in this context must respect the general principles of law*

and must not be irreversible. Emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period."

What is clear, is that the South African government did not wake up yesterday morning and decide it was going to start tracking and tracing people, it was clearly planning this from last week. On 26 March 2020, it published directions (a sort of lesser law) that obliges telecommunications service providers such as MTN, Vodacom and Cell C, to provide assistance with the tracking and tracing of people. The directions, called the Electronic Communications, Postal and Broadcasting Directions, say that telecommunications service providers and the "*internet and digital sector in general, must provide location-based services in collaboration with the relevant authorities identified to support designated departments to assist and combat the spread of COVID-19*."

What is important though, is that the State cannot simply implement this directive, without considering best practice that has been developed in other jurisdictions. The EDPB gives a good example of what is probably best practice. It highlights three important principles: Personal data that is used to achieve the directive's objectives should be processed for specific and explicit purposes i.e. fighting the Covid-19 pandemic. People should be given transparent information on how their data is being processed e.g. how long their personal data will be kept and what it will be used for. Crucially, because of the immense harm that can happen to people if personal data, such as their location, is leaked, adequate security measures and confidentiality policies must be adopted to ensure that personal information is not disclosed to unauthorised parties. The EDPB concludes by saying that it is important that measures that are implemented to manage an emergency such as the Covid-19 national disaster and the decisions on which they are based, should be appropriately documented.

This is not rocket science and is not new to the South African government. In a recent court ruling involving the State's collection of personal information using the Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA), *Amabhungane v Minister of Justice and Correctional Services*, the Judge held that the manner in which the State collected and held personal information, usage and accessibility controls and its integrity-oversight model were inadequate. For example, Amabhungane argued that there were inadequacies in where intercepted information was stored and who may have access to it. The Judge agreed that RICA did not prescribe sufficient procedures to follow when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions.

In dire circumstances such as these, even the most ardent proponent of privacy rights will concede that the appropriate use of location data, to combat Covid-19, is justified. The State just needs to assure us that the way it will collect the location data, what it will do with it, how long it will keep it and how securely it will be kept, will be in accordance with international best practice. Of course, if we all stay home, stay safe and avoid contracting Covid-19, then there may not be any need for the State to collect our location data…we hope.

Post Script

With the law changing so fast, further regulations were published on 2 April 2020. These regulations, amended the earlier regulations by inserting a new Chapter 3. This new chapter deals with the mechanics of what has been referred to as "*Contact Tracing*". As discussed above, tracking and tracing can be justified, provided that the precautions that have been listed, are implemented.

Whilst from face value, and given the limited time within which these Contact Tracing Regulations could be considered, they appear reasonable, one concerning aspect stood out. The Contact Tracing Regulations require the Covid-19 Tracing Database to be de-identified within 6 weeks of the end of the National State of Disaster and all information which has not been de-identified must be destroyed.

“De-identified” has many interpretations and if not undertaken properly, could result in those individuals on the data base eventually being capable of being identified.

If there is one aspect the State has to be absolutely transparent on, it is how the Covid-19 Tracing Database will be de-identified and whether it means permanently incapable of being re-identified.

You can access a copy of the Contact Tracing Regulations here .