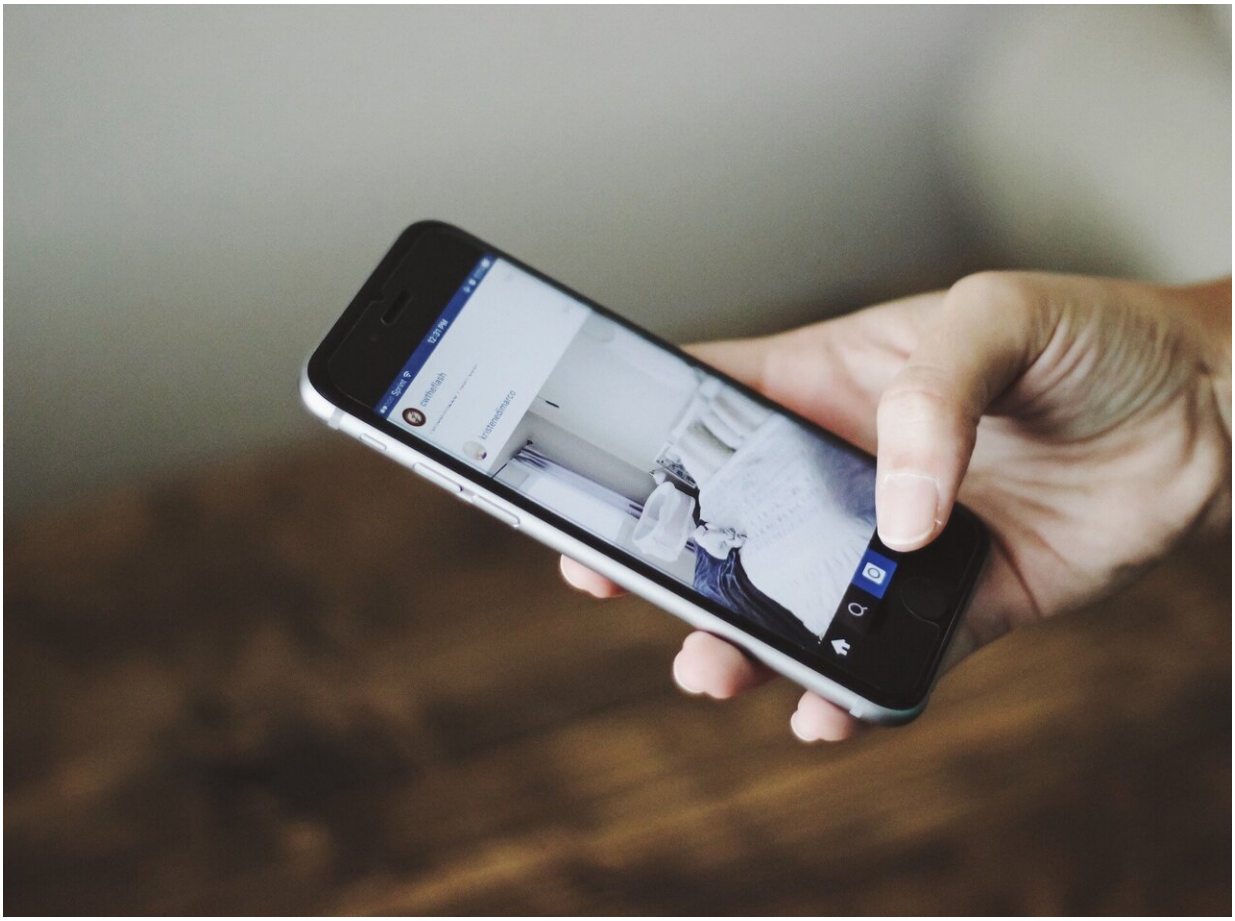
Mobile phone data is useful in coronavirus battle. But are people protected enough?

April 27 2020, by Alison Gillwald, Andrew Rens, Anri Van Der Spuy and Gabriella Razzano



Credit: CC0 Public Domain

Tracking people infected with COVID-19 has become an important

weapon in global responses to combating the virus. Through the use of geo-location, mobile technology offers a simple solution for tracing people possibly exposed to COVID-19. With big data analytics there is the potential for tracking the pandemic's spread, and employing analytics to forecast future patterns of contagion.

But at what cost? These are exceptional times calling for extraordinary measures. But do they justify the wholesale sacrifice of our rights? Concerns loom large across the globe. More than 100 civil society signatories and intergovernmental organizations have already warned as much in a joint letter.

The mobile phone industry is reportedly exploring the creation of a global data-sharing system that could track individuals around the world. For now, however, monitoring appears to be happening at national-level.

South Africa has joined several governments in passing regulations that allow the collection and storage of data from mobile companies. It has also appointed a former Constitutional Court Justice, Kate O'Regan, as the COVID-19 Judge. Her job will be to oversee data collection for the country's contact-tracing database led by the Director-General of Health, Dr. Anban Pillay.

The appointment of O'Regan indicates that the country is taking seriously concerns about the risks that monitoring can pose for human rights. Nevertheless, concerns remain about the ability of the Judge (or Parliament, which ultimately has oversight) to ensure that data, once collected, is not abused.

Global responses

A set of principles and 'best practices' have emerged internationally to guide data collection in disaster conditions. These include that:

- measures are transparent and accountable;
- the limitations of rights are proportional to the harms they are intended to prevent or limit;
- data collection is minimized and time constrained;
- data is retained for research or public use purposes and unused personal data is destroyed;
- data is anonymized in such a way that individuals cannot be reidentified; and
- third party sharing both within and outside of government is prevented.

However, South Africa's data protection framework is not yet in place. Large parts of the Protection of Personal Information Act, 2013 have not yet come into force. The Office of the Information Regulator has been established. And three years ago Advocate Pansy Tlakula was appointed Chairperson. But key sections of the Act are not in play. Thus, her powers to act are constrained.

There is synchronicity, however, between the principles and requirements of the COVID-19 regulations, and the lawful data processing principles the Act describes.

The Regulator has issued guidelines for the collection of data to manage and curb the spread of COVID-19. These guidelines are contained in the Disaster Management Act (Regulations). And she has called for proactive compliance by responsible parties when processing personal information of data subjects who have been tested for, or are infected with, COVID-19.

The guidelines confirm the powers of the state to conduct mass surveillance of both COVID-19 carriers, and potential carriers through the sharing of data by mobile operators. They also include reference to some of the privacy touchstones in data collection, particularly when

consent is not obtained.

The scope

Amendments to the disaster management regulations empower the Director-General of Health, to direct without prior notice, an electronic communications service provider to provide him with information for the COVID-19 tracing database to facilitate COVID-19 monitoring.

But these powers are circumscribed.

The regulations allow for the collection of location data of any person (and their personal identifiers) reasonably suspected to have contracted COVID-19, or that may have come into contact with someone who has. The commencement date is 5th March 2020.

The contents of the communication may not be intercepted by the Director-General—or anyone else.

The regulations state that the Department of Health will keep the information 'confidential." But big questions remain about the practical realities of ensuring that data remains secure, especially considering the Department's own tenuous history in relation to data protection.

The regulations empower the Director General to instruct a mobile operator to provide the information mentioned. But the actual modalities of the data collection by the Health Department is less clear—particularly how the data is collected and transmitted to the database securely.

For instance, once a request for the data from an operator is made and provided to the Director-General, who will receive the information to inform the contacts? Who will ensure they are tested?

Importantly the regulations limit the collection of data only to the purpose of addressing, preventing, or combating the spread of COVID-19. The data collected may only be disclosed by authorized persons for this purpose.

The Director-General is required to file weekly reports stating the number, names and details of all persons whose location or movements were obtained to the designated Judge. This will contribute to the oversight of collection. It will also go some way to constraining data collection to what's strictly necessary.

The duration of data collection is circumscribed and terminates with the end of the national state of disaster. And within six weeks of it lapsing, the Director-General is required to file a report with the COVID-19 Judge detailing steps taken to de-identify the data. This includes providing notifications to every person whose information was obtained.

The regulations require that all information on the COVID-19 Tracing Database, which has not been de-identified, be destroyed once the state of disaster has ended. But de-identification is not defined. This is a major concern, given the very real possibility of re-identification with the use of other publicly available, or hacked, databases.

Possible improvements

These measures go some way to safeguarding South Africans' individual rights while acting in the public interest to contain the virus.

But the regulations could be improved by:

- requiring that data subject be informed as soon as they are tracked, but no later than six weeks after the termination of the state of disaster;

- explicitly empowering the Judge to appoint technical experts to assist her in reviewing the use of data. This could include helping to ensure its security;
- explicitly giving the Judge access to the database and the data supplied by the cellular providers to verify reporting. This could also assist in monitoring security and other data processing protection measures;
- requiring immediate notification of all compromises of privacy or security of the data to the persons whose data is compromised; and
- clearly prescribing data processing standards that respect the principles set out in the Act.