# 10 Can we trust Big Brother? A critique of data protection measures in South Africa's COVID-19 tracing database

*Dusty-Lee Donnelly*

## Abstract

This chapter scrutinizes the South African government's response to the COVID-19 pandemic, focusing on data collection and the establishment of a COVID-19 tracing database under the Disaster Management Act. Critically analysing the regulations, it underscores sweeping provisions and inadequate guidance from the Information Regulator, especially regarding location tracking. The chapter provides an in-depth examination of POPIA's key principles – accountability, reasonableness, minimality, purpose specification, storage limitation, openness, and data subject participation – highlighting their application in the context of pandemic-driven data governance.

A trenchant critique explores the illusion of anonymization as a safeguard and cautions against unwarranted mass surveillance, raising concerns about citizens' privacy protection. The chapter concludes by contemplating the future of COVID-19 research, examining legal pathways for conducting scientific research under POPIA. It analyses the exemption from informed consent requirements in sections 15 and 27(1)(d), comparing it to the more stringent provisions of the public interest exemption in section 37, and questions whether adequate measures were taken to safeguard citizen privacy amidst the pandemic's data-driven response.

## 1 Introduction

On Thursday 5 March 2020 the first positive result for severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) was identified by the National Institute for Communicable Diseases in a small town in KwaZulu-Natal. COVID-19 had arrived in South Africa.

To keep the public informed of developments, the then Minister of Health, Dr Zweli Mkhize, issued a press briefing on the same date.[1] He did

1 National Institute for Communicable Diseases 'First case of COVID-19 coronavirus reported in SA' 5 March 2020, https://www.nicd.ac.za/first-case-of-covid-19-coronavirus-reported-in-sa/ (accessed 11 October 2021).

not name the patient, but provided enough personal information about the patient[2] that within a day the patient, his family, their doctor, the name of the town where they lived, and the school attended by their children were public knowledge.[3] While there were regrettable reported incidents of hate mail directed at the couple, the provision of clear information was critical when very little was known of the virus, and the potential for the public to panic was extremely high.

This incident brought into sharp focus the dichotomy between the right to privacy and the public's interest in a free flow of information about the virus and its spread. Section 2 of the Protection of Personal Information Act 4 of 2013 (POPIA) makes it clear that the Act is not focused solely on the protection of individual privacy but aims to strike a balance between the protection of privacy, through safeguarding personal information, and the protection of other rights, such as the right of access to information, and vital interests such as the free flow of information within and across our borders.[4]

While data protection laws are nothing new, the scale and speed of transition to widespread reliance on digital data processing during the COVID-19 pandemic makes a fresh analysis of data protection measures all the more urgent. The glut of digital data available today, and new computational techniques for the analysis of 'big data' using complex algorithms and artificial intelligence, have set new precedents in the public health and research sector. Likewise, restrictions on movement have meant that digital platforms have played an exponentially important role in all areas of work, education, and social life.

This chapter will discuss the South African government's use of data, including mobile-location data, to track citizens and monitor the spread of COVID-19. The government passed regulations under the

2 As defined in sec 1 of the Protection of Personal Information Act 4 of 2013 (POPIA). The personal information supplied included the patient's age, general, marital status, number of children, most recent travel location and number in the travel party, and the patient's medical history (symptoms, date and nature of treatment).

3 K Singh 'Coronavirus: Authorities pull out all stops, high-level meeting planned with KZN school' 6 March 2020, https://www.news24.com/news24/SouthAfrica/News/coronavirus-authorities-pull-out-all-stops-high-level-meeting-planned-with-kzn-school-20200306 (accessed 11 October 2021).

4 POPIA sec 2(a) reads: 'The purpose of this Act is to (a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at (i) balancing the right to privacy against other rights, particularly the right of access to information; and (ii) protecting important interests, including the free flow of information within the Republic and across international borders.'

Disaster Management Act[5] that provided for the creation of a COVID-19 'contact-tracing' database. Although 'contract tracing' is not defined in the regulations, it refers to the process of tracking and monitoring individuals who may have come into contact with a person infected with COVID-19. The objective of contact tracing is to notify individuals of their exposure (that is, close contact) to a known or suspected COVID-19-positive patient, thus breaking the chain of transmission as soon as possible.[6]

There is scientific support for the use of mobile location data to track and forecast the spread of COVID-19,[7] building on earlier studies that had begun to use mobile location data in response to Haiti's cholera outbreak in 2010[8] and the spread of the Ebola virus and Zika virus.[9] However, the absolute imperative of accurate real-time monitoring to track the spread of the virus and monitor the efficacy of interventions cannot overshadow the need for caution. In any instance where a government employs mass surveillance of its citizens, it must ensure that it does not do so 'for purposes unrelated to the pandemic'[10] and acts with due regard for the right to privacy.

## 2 Government response to COVID-19

COVID-19 soon spread rapidly in South Africa. In response to the pandemic, the government declared a state of national disaster on 15

5 Act 57 of 2002.

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' 21 April 2020 3, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en (accessed 11 October 2021).

7 I Marcello & E Vayena 'On the responsible use of digital data to tackle the COVID-19 pandemic' (2020) 26 *Nature Medicine* 463, describing a study that forecast COVID-19 spread using location-services data collected by the WeChat app, in combination with the Official Aviation Guide, a worldwide database of airline booking schedules. See JT Wu and others 'Nowcasting and forecasting the potential domestic and international spread of the 2019-nCoV outbreak originating in Wuhan, China: A modelling study' (2020) 395.1022 *The Lancet* 689.

8 L Bengtsson and others 'Using mobile phone data to predict the spatial spread of cholera' (2015) 5 *Scientific Reports* 1. The study collected anonymised data of the location of the last outgoing call or text message each day for 2,9 million users of Haiti's largest mobile operator over a period of two months.

9 M Bates 'Tracking disease: Digital epidemiology offers new promise in predicting outbreaks' (2017) 8 *IEEE pulse* 18. Web-based 'bio-surveillance' uses a variety of techniques to mine information on the web, such as news reports, Twitter and other social media posts, and web searches, to track or forecast disease spread.

10 United Nations 'COVID-19: We are all in the this together' April 2020 3, https://www.un.org/victimsofterrorism/sites/www.un.org.victimsofterrorism/files/un_-_human_rights_and_covid_april_2020.pdf (accessed 11 October 2021).

March 2020.[11] On 18 March 2020 the government issued the first tranche of regulations under section 27(2) of the Disaster Management Act 57 of 2002 (Regulations).[12] On 23 March 2020 the President of the Republic of South Africa announced that the National Coronavirus Command Council had decided to enforce a nation-wide lockdown.[13] At the time of writing, South Africa has been in lockdown, at varying levels of restrictiveness, for 19 months. The latest extension of the national state of disaster runs until 15 November 2021, with no indication of when or how it will finally be brought to an end.[14]

## 2.1 Collection of COVID-19 data

Almost immediately, the government set up a high-level advisory panel of scientific experts to develop evidence-based responses to the pandemic,[15] and from the outset there was a strong focus on collecting data from several sources. Twenty-eight thousand community health workers were re-deployed to do door-to-door visits to identify COVID-19 symptomatic cases, refer for testing and monitor compliance with quarantine restrictions.[16] During these screening visits, a mobile phone application, Covid Connect, was used to upload household data, symptoms and location coordinates to a central database and thus enable accurate mapping of screening coverage.[17] While community screening was rapidly criticised as unsustainable and unreliable given the high levels of asymptomatic patients,[18] it was reported that over 11 million people (around 20 per cent

11 Minister of Cooperative Governance and Traditional Affairs, Dr NC Dlamini-Zuma 'Disaster Management Act, 2002, Declaration of National State of Disaster' Gov Notice 313 in *Government Gazette* 43096 of 15 March 2020.

12 Minister of Cooperative Governance and Traditional Affairs, Dr NC Dlamini-Zuma 'Disaster Management Act, 2002, Regulations issued in terms of section 27(2)() of the Disaster Management Act, 2002' Gov Notice 318 in *Government Gazette* 43107 of 18 March 2020.

13 President of the Republic of South Africa, C Ramaphosa 'Statement by President Cyril Ramaphosa on Escalation of Measures to Combat COVID-19 Epidemic' 23 March 2020, http://www.dirco.gov.za/docs/speeches/2020/cram0323.pdf (accessed 11 October 2021).

14 Minister of Cooperative Governance and Traditional Affairs, Dr NC Dlamini-Zuma 'Disaster Management Act, 2002, Extension of a National State of Disaster (COVID-19)' Gov Notice R1031 in *Government Gazette* 45313 of 13 October 2021.

15 SS Abdool Karim 'The South African response to the pandemic' (2020) 382 *New England Journal of Medicine* e95.

16 As above.

17 As above.

18 M Mendelson & S Madhi 'South Africa's coronavirus testing strategy is broken and not fit for purpose: It's time for a change' (2020) 110 *South African Medical Journal* 429.

of the population) had been screened,[19] raising questions about the privacy and security of the data collected.

Free mobile tools for voluntary self-screening emerged,[20] and mandatory screening was implemented for all employees entering places of work[21] and learners, teachers and visitors at schools.[22] In addition, mobile applications for receiving exposure notifications were soon launched for both iOS and Android devices,[23] with mixed reviews regarding their privacy assurances[24] and efficacy as contact tracing tools.[25]

In addition, the results of all positive COVID-19 diagnostic tests[26] and rapid screening[27] in both the private and public sectors were communicated to the National Health Laboratory Service (NHLS).[28] These results were used to identify localised outbreaks and map hot spots for targeted lockdown regulations.[29] While the accuracy of the geo-spatial mapping of viral spread in real-time was severely hampered by delays in laboratory

19 Abdool Karim (n 15).

20 Business for SA 'South Africans encouraged to use COVID-19 digital health assessment tool' 8 June 2020, https://www.businessforsa.org/south-africans-encouraged-to-use-covid-19-digital-health-assessment-tool/ (accessed 11 October 2021). The National Department of Health made the symptom checker available using USSD via its dedicated COVID-19 Whatsapp chat service.

21 Minister of Employment and Labour, Thembelani Waltermade Nxesi 'COVID-19 occupational health and safety measures in workplaces' Gov Notice 479 in *Government Gazette* 43257 of 29 April 2021.

22 Department of Basic Education 'Standard Operating Procedures', https://www.nicd.ac.za/wp-content/uploads/2020/11/Revised-DBE-guidelines-Management-of-COVID-in-schools_Sept2020.pdf (accessed 11 October 2021).

23 D Johnson 'Assessment of contact tracing options for South Africa' (October 2020) Research ICT Africa Cape Town, https://researchictafrica.net/wp/wp-content/uploads/2020/10/Contact-tracing-survey-report-David-Johnson-Oct2020.pdf (accessed 11 October 2021).

24 L Bradford and others 'COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes' (2020) 7 *Journal of Law and the Biosciences* 34.

25 IM Viljoen and ohers 'Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa' (2020) 13 *South African Journal of Bioethics Law* 21 argue that it is not viable in South Africa where 'many people do not have smartphones'. For a full discussion of the barriers to uptake, including smartphone penetration, data costs and required download rates for effective contact tracking, see Johnson (n 23) 1-2.

26 The reverse transcriptasepolymerase chain reaction (RT-PCR) test.

27 SARS-COV-2 rapid antigen and antibody tests.

28 National Health Laboratory Service 'COVID-19 surveillance reports', https://www.nicd.ac.za/diseases-a-z-index/disease-index-covid-19/surveillance-reports/ (accessed 18 October 2021).

29 Abdool Karim (n 15).

test turnaround time and a lack of uniformity in rates of testing,[30] the National Department of Health has continued to provide the public with daily statistics of new infections and deaths and regular regional updates on testing, rates of infection, recoveries, deaths, and more recently, vaccinations.[31]

## 2.2 COVID-19 tracing database

Additional data collection measures were implemented from 2 April 2020, when a COVID-19 tracing database was created by amendment of the regulations.[32] The new regulation 11H made it mandatory for every person being tested for COVID-19 to disclose a set of personal information comprising the person's first name, surname, identity or passport number, residential address, other addresses at which the person could be located, cellular telephone number and a copy of photographic identification (such as identity book, identity card or passport). In addition, they were required to disclose the names and contact details of all persons with whom they had known or suspected close contact.[33] Every testing site was obliged to collect these particulars insofar as they were available when administering the test.[34] In every case of a positive COVID-19 result, the person's personal information, their result, and the personal information of their contacts are communicated by the laboratory and the NICD to the Director-General: Health for inclusion in the COVID-19 contact-tracing database.

The regulations also contained measures to monitor the movement of persons. The same set of personal information was to be collected for all persons staying at accommodation establishments set up for essential services workers, quarantine, isolation and those stranded under the hard lockdown (when travel restrictions prevented persons returning home in certain cases) and included in the database.[35] Furthermore, the Director-General: Health was authorised to requisition mobile-location data from electronic communication service providers regarding 'the locations or movements of any person known or reasonably suspected to have

30 Mendelson & Madhi (n18) 429.

31 National Department of Health 'COVID-19 online resources and news portal', https://sacoronavirus.co.za/ (accessed 11 October 2021).

32 Minister of Cooperative Governance and Traditional Affairs, Dr NC Dlamini-Zuma 'Disaster Management Act, 2002, Amended of regulations issued in terms of section 27(2)' Gov Notice R446 in *Government Gazette* 43199 of 2 April 2020.

33 Regulation 11H (3)(a)-(c).

34 Regulation 11H (6).

35 Regulation 11H (9) read with Annexure D to the regulations.

contracted COVID-19, and 'any person known or reasonably suspected to have come into contact [with them]'.[36] These were sweeping provisions that were rightly cause for close scrutiny.

## 2.3 Guidance from the Information Regulator

In response to the need for clarity on data protection issues, the Information Regulator of South Africa issued a guidance note on data protection during the pandemic on 3 April 2020.[37] At the time POPIA had not yet come into full force.[38] Nevertheless, the Information Regulator 'encourage[d] proactive compliance by responsible parties when processing personal information of data subjects who have tested or are infected with COVID-19, or who have been in contact with such data subjects'.[39]

At the same time the Information Regulator recognised that effective management of the spread of COVID-19 'has necessitated the limitation of various constitutional rights of data subjects', and 'supports the need to process personal information of data subjects in order to curb the spread of COVID-19'.[40]

While the Information Regulator's response was timely, it was disappointingly thin on detail. Although the guidance note recorded that the regulations should be implemented 'in conjunction with' the conditions for lawful processing of personal information[41] there was no actual guidance on the extent to which the regulations in fact complied with the conditions for lawful processing, or on whether limitations to the right to privacy were in fact constitutionally justifiable in scope.

36 Regulation 11H (10).

37 Information Regulator of South Africa '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 (POPIA)' 3 April 2020, https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf (accessed 11 October 2021).

38 The commencement of the operative provisions of POPIA took place on 1 July 2020 in terms of Proclamation R21 of 2020 in *Government Gazette* 43461 of 22 June 2020. In terms of sec 114(1) of POPIA a one-year grace period to bring all processing into line with the Act applied until 30 June 2021.

39 Information Regulator (n 37) para 2.1.

40 Information Regulator (n 37) para 2.3.

41 Information Regulator (n 37) para 9.

# 3 Protection of personal information

## 3.1 Processing health data as special personal information

Information pertaining to a data subject's health is included in the definition of special personal information.[42] Processing of such information is prohibited without a lawful ground of authorisation.[43] The first general authorisation for processing special personal information requires that the data subject (or their parent or guardian in the case of a child) has given consent for the processing.[44] However, a number of other general and specific authorisations for processing are set out.

In the context of the COVID-19 pandemic, the most relevant would be that the party was processing the personal information, including health information, in order to comply with a legal obligation imposed by the regulations.[45] The general authorisation for research conducted in the public interest is discussed later in this chapter. In addition, the processing of health data is specifically authorised by POPIA in a number of specific use cases, including patient treatment and care, and the administration of health care institutions,[46] and by insurance companies and medical schemes,[47] schools[48] and employers.[49]

## 3.2 Defining location information as personal information

POPIA includes 'location information' in the definition of personal information in section 1 of the Act. Such data must therefore be processed

42 POPIA sec 1.

43 POPIA sec 26.

44 POPIA sec 27(1)(a).

45 POPIA sec 27(1)(b) authorises the processing of any special personal information where the 'processing is necessary for the establishment, exercise or defence of a right or obligation in law'. Similarly, see the general justification for processing any other personal information under sec 11(1)(c).

46 POPIA sec 32(1)(a).

47 POPIA sec 32(1)(b), although a data subject's right to object to processing is specifically preserved in relation to the use of health data for purposes of 'risk assessment'.

48 POPIA sec 31(1)(c), insofar as is necessary to accommodate a pupil's special needs or make special arrangements concerning their health.

49 POPIA sec 31(1)(d). The provisions can be interpreted to include collection of health data where relevant to the administration of pension schemes and funeral benefits, as well as the support and reintegration arrangements made for workers self-isolating or with co-morbidities that might require special arrangements to work from home during the COVID-19 pandemic.

in full compliance with the conditions for lawful processing set out in the Act. The term 'location information' is not further defined in POPIA, but when read with the general definition of personal information, it should be interpreted to mean any data that reveals the geographic position of the data subject, with a sufficient degree of proximity that their identity can be revealed or it might reveal other personal information about them. For example, location information might reveal where a person lives or works, and a visit to a medical testing facility might reveal the data subject's medical history or likely medical condition.

In the COVID-19 context government tracked location information manually and electronically. Manual entries in paper-based or electronic patient health records at the time of any testing for COVID-19 included the patient's home address and recent close contacts, and were required by law to be transmitted with the patient's name, identity number, contact details and test results to the NICD. Both the NICD and the entity administering the test would be a responsible party and as such fully accountable for full compliance with POPIA in respect of its processing of that personal information.

However, the real concern was with location tracking of citizens in (near) real time using the location data collected by electronic communication service providers, such as mobile cellular network providers. The regulations[50] provided:

> The Director-General: Health may, in writing and without prior notice to the person concerned, direct an electronic communications service provider licensed under the Electronic Communications Act, 2005 (Act No 36 of 2005) to provide him or her, for inclusion in the COVID-19 Tracing Database, with such information as that electronic communications service provider has available to it regarding –
>
> (a) the location or movements of any person known or reasonably suspected to have contracted COVID-19; and
> (b) 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, with a person contemplated in subparagraph (a),
>
> and the electronic communications service provider must promptly comply with the directive concerned.

50 Regulation 11H (10).

In this context, the term 'location data' refers to information that reveals the geographic position of the user's device. This is still personal information as it may be inferred that the location(s) or movement(s) of the device provide information about the location(s) or movement(s) of the device user.[51] There are two principal ways in which mobile location data can be collected: mobile location tracking and network-based location tracking. In both cases, collection can be carried out at least partly undetected and is not well understood by device users, heightening mistrust.

### *3.2.1 Mobile location tracking*

Firstly, mobile applications installed on smart devices, such as smartphones and tablets, can track location using the on-device GPS sensor. An application user has some control over location tracking as they must grant an application permission to access location and can also turn off location services in the device system settings. What may be less clear to the application user is whether the application is monitoring location only when the application is in use, or continuously by way of a background process. Further application users may not understand the practical difference between the course-grained and fine-grained instantiation of location data collection by the application. Further, even if location services are turned off, it is possible to passively track location and the proximity of devices to one another, using wireless network (WLAN)[52] and Bluetooth[53] connections by collecting the identification code of the wireless access point or Bluetooth beacon and signal strength (as a proxy for proximity of the device and the duration of proximity).

These are the types of location information used by contract tracing mobile applications such as Covid Connect, COVI-ID and COVID-ALERT.[54] The privacy of users of such applications may differ greatly. For example, it is reported that in China the contact-tracing application 'Health Code' generates a code that is required to access homes, shopping centres, businesses and public transport. As using the application is mandatory, it

51 See eg the definition in the European Union's Privacy and Electronic Communications Directive 2002/58/EC. Art 2(c) and rec 14: 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.

52 See eg *United States v InMobi Pte Ltd* Case 3:16-cv-03474 (ND Cal June 22, 2016).

53 Bengtsson (n 8) 1.

54 Johnson (n 23) 20-23.

has 700 million users. GPS and Bluetooth location data are collected and the application reportedly shares this information with the police.[55]

In contrast, the COVID-ALERT application developed by the South African National Department of Health uses the exposure notification framework developed by Google and Apple. The application is designed to protect privacy by sending a randomised Bluetooth identification beacon (that changes every 10 minutes) to other devices in close proximity that also have the application installed. Data is stored on the user's device, not a central server, and is only stored for 14 days. A user, upon receiving a positive COVID-19 diagnosis, can then choose to upload the anonymous Bluetooth codes to the central server that would deliver them to every device that had registered them in the last 14 days. At no point is any person identified.[56]

### *3.2.2 Network-based location tracking*

Second, network-based location tracking refers to a form of location tracking enabled by cell site location information collected by cellular network operators (electronic communications service providers) through the continuous connection of the mobile phone to radio antennae positioned on cell towers, from which the mobile phone obtains its signal and on which its functionality depends.[57] While less accurate than GPS, being approximate to the radius of the tower's signal coverage,[58] by triangulating the signal, greater accuracy is obtained, and the connection automatically generates a time-stamped record of these connections.[59]

The term 'historical' or 'archived' cell site location information thus refers to this record of past movements, that is automatically being collected and stored about every cell phone user. The term 'real-time' data relates to tracking in the present moment on an ongoing basis.

55 M Wang 'China: Fighting COVID-19 with automated tyranny' *The Diplomat* 1 April 2020, https://thediplomat.com/2020/03/china-fighting-covid-19-with-automated-tyranny/ (accessed 18 October 2021).

56 National Department of Health 'COVID Alert SA app: Data protection and privacy policy', https://sacoronavirus.co.za/covidalert/privacy-policy/ (accessed 18 October 2021).

57 It is the form of tracking that led to the landmark US decision in *Carpenter v United States* 585 US (2018) which held that obtaining historical cell site location information without a warrant violated 4th amendment rights.

58 On average one to ten kilometres squared.

59 D Donnelly ' Privacy by (re)design: A comparative study of the protection of personal information in the mobile applications ecosystem under United States, European Union and South African law' PhD thesis, University of KwaZulu-Natal, 2020 79.

Access by law enforcement officials to the records stored by electronic communications service providers is controlled under the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA).[60] Nothing in the regulations is concerned with monitoring communications content,[61] which would remain governed by RICA. However, the regulations supersede the requirements for RICA insofar as they provide for the interception of real-time or archived location data ('communication-related information') without a RICA directive. Under RICA, if only archived communication-related information is required, a magistrate may issue the required directive,[62] whereas if real-time communication-related information is required on an 'ongoing basis', only a judge of the High Court can issue the directive.[63] If another Act makes provision for the interception of communications-related information, such information cannot be collected on an ongoing basis.[64] There are few exceptions. In situations of urgency, and only in order to prevent serious bodily harm, law enforcement officials can obtain interception of communications or indirect communications without a prior directive, provided that they present an affidavit to a High Court judge as required under RICA as soon as reasonably practicable thereafter.[65]

While the pandemic may have created grounds for extraordinary measures during the suspension of the ordinary democratic process, it is essential to closely scrutinise the national disaster regulations as they have dispensed with the requirement for an interception and monitoring directive and instead authorised the Director-General: Health to issue directives directly to electronic communications service providers to requisition network-based location information.

## 3.3 Accountability

The Information Regulator's guidance note addressed the question of whether an electronic communications services provider can share 'mobile location-based data of data subjects' with government for the purpose of tracking data subjects.[66] The question appears to be directed to the tracking

60 Act 70 of 2002.

61 Regulation 11H (12) provides: 'Nothing in this regulation entitles the Director-General: Health or any other person to intercept the contents of any electronic communication.'

62 RICA sec 19(1). These provisions are preserved by sec 40(2) of the Cybercrimes Act 19 of 2020.

63 RICA sec 17(1).

64 RICA sec 15(2).

65 RICA secs 7(1) & (2).

66 Information Regulator (n 37) para 5.1.

of an identifiable data subject, and reference to 'mobile location-based data' probably refers to the provision of network-based location data by electronic communications services providers, but could include location tracking by mobile applications. In this context, it must be assumed that the location data has not been de-identified and must be processed in full compliance with POPIA.

A responsible party is defined under section 1 of POPIA as 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information'. Thus, each entity that collected personal information would be regarded as a responsible party. In addition, the National Department of Health, as the recipient of the location information, is a responsible party in respect of its storage of the data in the COVID-19 tracing database and its use of the data for monitoring COVID-19. As such, the Director-General: Health must ensure compliance with all eight conditions of lawful processing for the entire lifecycle of the data (from receipt until destruction or de-identification of the data).

## 3.4 Processing limitation: Lawful justification

Any collection and transfer of personal information by collection and testing sites and electronic communications services provider to the Director General: Health falls within the definition of 'processing' under POPIA and, as such, requires a lawful justification under section 11 of the Act. While consent of the data subject is the first basis for lawful processing, it is not the only permitted ground. As the regulations imposed duties upon all persons collecting and testing samples to collect and transfer the information they would, as responsible parties under POPIA, be able to rely on subsection 11(1)(c) in that 'processing complies with an obligation imposed by law on the responsible party'. The data subject has no right to object to such processing.[67] The processing by public bodies such as the National Department of Health could also be justified under subsection 11(1)(e) which provides for processing that 'is necessary for the proper performance of a public law duty by a public body'. Processing could also be justified as being in the legitimate interests of the National Department of Health, as the party receiving the data,[68] or even in the

67 POPIA sec 11(3)(a) provides: 'A data subject may object, at any time, to the processing of personal information (a) in terms of subsection (1)(d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, *unless legislation provides for such processing*'.

68 POPIA sec 11(1)(d).

'legitimate interests of the data subject' to know if they have contracted or been exposed to COVID-19.[69]

However, POPIA does not simply require a lawful justification for processing. It also imposes a requirement that processing should be reasonable and respect the data subject's privacy.

## 3.5 Reasonableness and the right to privacy

Section 9 of POPIA requires that all processing must be undertaken 'in a reasonable manner that does not infringe the privacy of the data subject'.[70] In general, the disclosure of a person's identity might constitute a breach of the right to privacy in certain circumstances.[71] Not all personal information will be the kind of private facts and private documents that enjoy protection under the right to privacy.[72] However, the data being collected for the COVID-19 tracing database clearly is private information and must be accordingly handled with appropriate safeguards.

An individual's medical records, such as the results of a COVID-19 test being entered in the COVID-19 tracing database, are sensitive and personal information that is private and confidential.[73] Disclosure is ordinarily strictly regulated by the National Health Act.[74] Where disclosure takes place in accordance with law, our courts have found that there is no invasion of privacy and no breach of POPIA,[75] but such cases require careful attention to the constitutionality of the law and whether it has been complied with.[76]

69 POPIA sec 11(1)(b).

70 POPIA sec 9(b).

71 *Bernstein & Others v Bester & Others NNO* 1996 (2) SA 751 (CC) para 58. The Court provides an extensive discussion of the right to privacy from para 65 onwards.

72 Constitution of the Republic of South Africa 1996, sec 14.

73 *Tshabalala-Msimang & Another v Makhanya & Others* 2008 (6) SA 102 (W) para 26 onwards.

74 Act 61 of 2003 sec 14, which will be applied together with any applicable law relating to discovery or compulsion of evidence in civil and criminal proceedings. See *Unitas Hospital v Van Wyk & Another* 2006 (4) SA 436 (SCA) para 21; *Industrial Development Corporation of South Africa Ltd v PFE International Inc (BVI) & Others* 2012 (2) SA 269 (SCA) 275B-C.

75 *Divine Inspiration Trading 205 (Pty) Ltd & Another v Gordon & Others* 2021 (4) SA 206 (WCC).

76 This chapter will not conduct an analysis of the constitutionality of the regulations. The unfortunate judgment in *De Beer & Others v Minister of Cooperative Governance and Traditional Affairs* 2020 (11) BCLR 1349 (GP) was swiftly set aside in *Minister of Cooperative Governance and Traditional Affairs v De Beer & Another* [2021] 3 All SA 723 (SCA), with the SCA cautioning at para 2 that any constitutional challenge should be approached in a disciplined and cautious manner.

The location information being collected for the COVID-19 tracing database must also be treated as private. Evidence presented in the case of *Carpenter v United States*[77] revealed just how privacy-invasive such digital shadowing can be. Authorities had collected 12 898 time-stamped location points recording Carpenter's movements over 127 days – an average of 101 data points per day. The United States Supreme Court found that this was a clear invasion of privacy as it creates an 'intimate window' into an individual's life, 'revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations"'.[78]

As such, the regulations pertaining to the COVID-19 database must be carefully analysed to determine whether they provide for full compliance with all conditions for lawful processing, or whether their implementation would result in an infringement of privacy that will *ipso facto* be unreasonable for the purposes of section 9 of POPIA.

## 3.6 Minimality

The processing limitation and reasonableness requirement are further embodied in the principle of 'minimality'. POPIA provides that '[p]ersonal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive'.[79] In this regard the regulations fall short.

Viljoen and others note that since network-based location information cannot identify a close contact (as it does not have the pinpoint accuracy of GPS location information) the use of such a 'technically inappropriate method [is] questionable'.[80] On this basis I would argue that the adequacy and relevance of the location data for the specified purpose have not been made out.

Furthermore, the scope of data collection is potentially excessive. The regulations stipulate that such information can only be requested 'during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated'.[81] However, what is absent from the regulations is any indication of the time frame for which location data can be collected about a particular individual. On the face of it, the Director-

77 *Carpenter* (n 57) 3.

78 *Carpenter* (n 57) 12, citing *United States v Jones* 565 US 400 415.

79 POPIA sec 10.

80 Viljoen and others (n 25) 21.

81 Regulation 11H (11)(a).

General: Health may direct electronic communication service providers to transfer mobile-location data on every person whose details were collected under the regulation on an ongoing basis throughout the national state of disaster.

To be lawful in terms of their own stated purpose, however, the regulations must be interpreted as impliedly limiting the collection of such data to specific persons whose contacts needed to be traced, and for a limited period that could be scientifically justified as necessary for contact tracing. This would mean that mobile-location data could only be relevant to contact tracing in relation to a person after a positive test result was confirmed for that person and in instances where there was no other reliable information about that person's current location, or about their contacts during the period they were known or suspected to have been infectious. Given that the Regulations appear to authorise the Director-General: Health to requisition the details of any person who was tested (even before the result of their test was known)[82] and all their reported known or suspected contacts, a further implied limitation should be read in that the information obtained will not be entered automatically into the COVID-19 tracing database. If the test result is subsequently negative, or if reliable contact details have been provided, the data should be deleted.

It follows that to comply with the minimality principle, only historical mobile-location for a reasonable number of days prior to testing during which the person may have been infectious could be justified. To ensure compliance with the principles of lawfulness, transparency and data subject participation the regulations ought to have specified this period.

The regulations do not do this, referring widely to '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, with a person contemplated in subparagraph (a)'.[83]

Clearly, on face value this cannot be interpreted as permitting ongoing location tracking of any single individual for the entire period. Ongoing monitoring of the location of an individual would be a clear invasion of privacy that would be grossly disproportionate to the lawful object of the

82 Regulation 11H(10)(a) refers to 'the location or movements of any person known or *reasonably suspected* to have contracted COVID-19'. The determination that there is a known or reasonably suspected case of COVID-19 is made by the DG Health, but must be objectively reasonable on a sound scientific basis..

83 Regulation 11H(10)(b).

regulations, and never justifiable when one considers the stated purpose of the regulations.

## 3.7 Purpose specification

POPIA requires that any responsible party processing data must have 'a specific, explicitly defined and lawful purpose' for collecting the data,[84] and this purpose then acts as a brake on further processing, which must always be compatible with the original purpose of collection, unless a new ground of justification can be established.[85]

The regulations' stated purpose for the processing of mobile location data was clearly expressed. The information 'may only be obtained, used and disclosed when necessary for the purposes of addressing, preventing or combatting the spread of COVID-19 *through the contact tracing process'*.[86] This is a significant safeguard protecting against 'function creep', where data is used for a purpose for which it was not originally collected.[87] It is clear from the regulations that they do not permit transfer of the data collected for the COVID-19 tracing database to other government departments, such as the police,[88] or to private bodies, such as employers.[89]

The regulations ought to have also contained a specific indication of whether any mobile-location data could be collected about an individual after their positive test result, and if so this should have been limited to the number of days they were likely to remain infectious. Even if the regulations had contained such a limitation the rationale for such collection would be much weaker, as a person who has tested positive would be self-isolating or in a quarantine facility. The regulations were expressly limited to what was necessary for *contact tracing*, and did not authorise the collection of information to monitor quarantine compliance.

84 POPIA sec 13(1).

85 POPIA sec 15(1).

86 Regulation 11H (11)(b) (my emphasis).

87 Bradford (n 24) 11.

88 N Sun and others 'Human rights and digital health technologies' (2020) 22 *Health and Human Rights Journal* [special section 'Big Data, Technology, Artificial Intelligence and the Right to Health'] 22.

89 As to the position of employees generally, see DT Hagemeister and others '"Please confirm your HIV-positive status by email to the following government address": Protection of "vulnerable employees" under COVID-19' (2020) 13 *South African Journal of Bioethics and Law* 91.

Moreover, ongoing monitoring of location data for an unspecified period would, I argue, never be justified.

## 3.8 Storage limitation

POPIA provides that 'records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed'.[90] Although POPIA contains an exception where 'retention of the record is required or authorised by law' or when 'the responsible party reasonably requires the record for lawful purposes related to its functions or activities',[91] these would still be subject to the requirement of reasonableness in section 9.

The regulations provide two different storage limitations. First, data not included in the COVID-19 tracing database 'may only be retained by the Director-General: Health for a period of six weeks after being obtained and shall thereafter be destroyed'.[92] However, this limitation will not apply in many cases, as mobile-location data 'where relevant to the contact tracing process, must be included in the COVID-19 tracing database'.[93] Data in the database will be retained in a personally-identifiable form until the end of the national state of disaster, after which it must be de-identified within six weeks.[94]

If the data has been de-identified, it will no longer be personal information, and it 'shall be retained and used only for research, study and teaching purposes'.[95] As de-identified data is no longer subject to POPIA, it can be retained indefinitely. If it is not de-identified, it will be destroyed.[96] Given the importance of protecting privacy, it is welcome that the regulations contain a restriction on the purpose for which de-identified data may be used, although the scope of such purpose remains broad. It is further welcome that the measures taken must be reported to the COVID-19 judge. However, it is to be hoped that the judge recommends scrutiny of the data by a professional qualified to determine whether the data has been de-identified and that there is no reasonable risk that it could be reconstructed or linked with other data to re-identify individuals. Collection of mobile location data on a large scale or for an extended

90 POPIA sec 14(1).
91 POPIA secs 14(1)(a) & (b).
92 Regulation 11H (11)(d).
93 Regulation 11H (11)(c).
94 Regulation 11H (17)(a).
95 Regulation 11H (17)(b).
96 Regulation 11H (17)(c).

period, even if it will subsequently be anonymised, would not meet the conditions for lawful processing under POPIA.

## 3.9 'Anonymous' mass surveillance

The Regulator's guidance note addressed a second question, namely, whether an electronic communications service provider can share location-based data with the government 'for the purpose of conducting mass surveillance of data subjects' in its COVID-19 response.[97] Here the Regulator's position was that this is only permissible 'if the personal information is anonymised or de-identified in a way that prevents its reconstruction in an intelligible form'.[98]

The recommendation lacked any teeth since POPIA only became binding on 1 July 2021 but, more to the point, it should have raised alarm bells about whether, and by what means, 'mass surveillance' was taking place when (as set out above) such measures were not contained within the purpose of the regulations as framed. Second, it should have fully addressed what is required for de-identification of data.

Truly de-identified data serves no purpose for contact tracing – the stated purpose of the regulations. Although governments around the world conceived large-scale monitoring of aggregated location data as helpful for modelling the spread of the virus and thus assessing the effectiveness of lockdown restrictions in slowing or containing the pandemic,[99] these aims were not addressed in the regulation's stated purpose. Thus, no matter how useful this information may be, the regulations did not permit its collection, even in an anonymous form.

Second, to regard data as anonymous a strict test must be applied. Anonymisation, or de-identification as it is termed in POPIA, refers to the principle that data is de-identified when it cannot directly or indirectly identify an individual. There must be 'no reasonably foreseeable means of reversing the de-identification (re-identifying the information), or linking the information to other information and in that way identifying the data subject'.[100] This principle is expressed in slightly different but consistent

97 Guidance note (n 37) para 5.2.

98 As above.

99 European Data Protection Board (n 6) 5 recommended that preference always be given to anonymised data over personal data.

100 Donnelly (n 59) 79.

ways in most data protection statutes around the world.[101] These include Recital 26 of the General Data Protection Regulation 2016/679 (GDPR) in the European Union (EU)[102] and section 164.514 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA privacy rule) in the United States.[103]

The critical attribute of de-identified data is not only that it has been irreversibly stripped of direct identifiers but that there is no reasonable possibility that an individual can be re-identified by manipulating the data or linking it to other data. As the European Data Protection Board has explained, reasonableness in this context refers to both general objective criteria such as the currently available technology and time required for re-identification, and to the specific circumstances of a particular case where, for example, the rarity of a phenomenon or scarcity of data may make it more likely that a particular individual can be identified.[104]

A growing body of research has shown that re-identification attacks can be performed with relative ease and that mobile location data is particularly vulnerable owing to the uniqueness of an individual's 'mobility traces'.[105] For example, anonymised location data with four spatio-temporal points can identify 95 per cent of individuals from their pattern of movements,[106] and one study showed that 99,9 per cent of individuals in the state of Massachusetts could be correctly re-identified from an anonymised dataset containing only 15 demographic variables.[107]

This means that the protection offered by an assurance that data will be de-identified is highly dependent on the techniques used to anonymise the data. POPIA, being technologically neutral principles-based legislation,

101 L Swales 'The Protection of Personal Information Act and data de-identification' (2021) 117 *South African Journal of Science* 1.

102 General Data Protection Regulation: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016.

103 Health Insurance Portability and Accountability Act of 1996 PubL 104–191; 110 Stat 1936.

104 European Data Protection Board (n 6) 5.

105 As above.

106 Y de Montjoye and others 'Unique in the crowd: The privacy bounds of human mobility' (2013) 3 *Scientific Reports* 1.

107 L Rocher and others 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019) 10 *Nature Communications* 5.

does not specify any particular anonymisation technique. However, there is no reason why the regulations, if they intended to authorise the collection of aggregated location data, should not have set out both the requirement for it to be de-identified, as well as steps to be taken by the electronic communications service provider to confirm that the data was de-identified before it was transferred.

The danger of referring to data as anonymous is that it then falls outside the ambit of POPIA. Too ready reliance on anonymisation as a safeguard could lead governments to act with impunity and disregard POPIA altogether in the belief that the Act does not cover the data. Given the difficulty of genuinely anonymising data, it should rather be treated as pseudonymised and then handled subject to POPIA with due regard for the data subject's right to privacy and the obligations to ensure the security and integrity of the data.

## 3.10 Security

The regulations outline, in broad strokes, the protection of the confidentiality of the data collected.[108] If those assurances are to offer solace, they must be operationalised by technical and organisational measures to limit access to the data to authorised persons only and guard against loss, damage, or unauthorised destruction of the data.[109] The servers on which it is stored, the devices on which it is accessed, and the applications or networks through which it is transmitted must all be secure,[110] and measures must be in place to ensure that unauthorised access to data is swiftly detected and that data breaches are promptly reported.[111] While it may be sufficient to detail such measures in internal policies and procedures and not in the regulations themselves, the lingering concern remains that 'not enough

108 Regulation 11H (11) provided that the location data referred to in sub-regulation (10) 'may only be obtained, used or disclosed by authorised persons'. Further sub-regulation (4) stipulated that all information in the COVID-19 tracing database or obtained under the regulations is confidential. In terms of sub-regulation (5): 'No person may disclose any information contained in the COVID-19 tracing database or any information obtained through this regulation unless authorized to do so and unless the disclosure is necessary for the purpose of addressing, preventing or combatting the spread of COVID-19.'

109 POPIA sec 19(1).

110 Viljoen and others (note 25) 23.

111 POPIA sec 22 read with sec 19(2) which requires ongoing monitoring to verify that safeguards have been implemented effectively, and sec 19(4).

attention has been given to exactly how confidentiality is protected, and what will happen if it is breached'.[112]

## 3.11 Openness and data subject participation

Even when consent is not relied upon as the legal justification for processing, the principle of openness requires that the data subject should ordinarily be notified about the processing.[113] Notice to the data subject should also inform them of any necessary information to render the processing reasonable, including informing them of their right of access to the data records held on them, and their right to rectify the information in those records.[114] It follows that the responsible party must make it possible for the data subject to exercise these rights. Under POPIA, non-compliance with section 18 is condoned only on reasonable grounds, including where 'compliance is not reasonably practicable in the circumstances of the particular case'.[115]

Under the regulations the Director-General: Health is authorised to requisition the information without prior notice to the persons concerned.[116] The regulations provide that every person whose information is obtained will be notified 'within six weeks after the national state of disaster has lapsed',[117] but there is no provision for access to or rectification of the data.

Electronic communications service providers were required to 'promptly comply' with any written directive from the Director-General. No appeal mechanism was created. Non-compliance is an offence for which a person is liable, on conviction, to a fine or imprisonment for up to six months, or both such fine and imprisonment.[118]

The regulations contain a significant safeguard for the constitutional right to privacy. Retired Constitutional Court Justice O'Regan was appointed[119] to receive weekly reports providing the names and details of all persons whose location and movements were obtained by the

112 Viljoen and others (n 25) 24.

113 POPIA sec 18(1).

114 POPIA sec 18(1)(h)(iii).

115 POPIA sec 18(4)(e).

116 Regulation 11H (10).

117 Regulation 11H (16).

118 Regulation 11I.

119 Regulation 11H (13), read with Government of South Africa 'Media statement' 4 April 2020, https://www.sanews.gov.za/south-africa/o%E2%80%99regan-appointed-covid-19-designated-judge (accessed 11 October 2021).

Director-General: Health.[120] The judge has the power to make such recommendations as she deems fit 'regarding the amendment or enforcement of this regulation in order to safeguard the right to privacy while ensuring the ability of the Department of Health to engage in urgent and effective contact tracing to address, prevent and combat the spread of COVID-19'. However, it does not appear that she has done so. She will also receive a final report that confirms the steps taken to notify every person whose location data was collected about that fact and the steps taken to destroy or de-identify the data,[121] and she may give directions as to any further steps that must be taken to safeguard the right to privacy.[122] Both the report and any directions given by the judge will be tabled in Parliament.[123] While the provision seems reasonable on the face of it, the longer the national state of disaster persists, the weaker the rationale becomes for not complying fully with POPIA.

## 4 Location monitoring and the public interest exemption

In view of the analysis that the regulations do not comply with POPIA it must be considered whether that non-compliance meets the grounds for an exemption. Although the power was not exercised during the COVID-19 pandemic, section 37(1) of POPIA empowers the Information Regulator to exempt a responsible party from compliance with a condition of lawful processing, in cases where:

> (a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or
> (b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.

The concept of public interest is a broad one that defies attempts at a precise or comprehensive definition.[124] Its core component is that the action should benefit the public by improving public welfare or services. On a narrow view, it suffices if the public at large can be said to enjoy

120 Regulation 11H (14).

121 Regulation 11H (17)(d).

122 Regulation 11H (18).

123 Regulation 11H (19).

124 *Rail Commuter Action Group & Others v Transnet Ltd t/a Metrorail & Others (No 1)* 2003 (5) SA 518 (C) 558A-B, and *Argus Printing and Publishing Co Ltd v Darbys Artware (Pty) Ltd* 1952 (2) SA 1 (C) 8-10.

the general benefit contemplated in the empowering legislation.[125] On a broad view, it means only that 'the public would be better off by having the service than by being without it'.[126] While the concept generally refers to the public at large, as opposed to a few or even a single person or entity,[127] in certain circumstances, the 'public' might properly refer only to a specific group or community.[128]

> Context matters. The Constitutional Court has held:[129]
>
> > Determining the scope of public power, therefore, and any duties attached to it requires an analysis not only of the statutory provisions conferring the power, but also of the social, political and economic context within which the power is to be exercised and a consideration of the relevant provisions of the Constitution. If this approach is followed, the ambit of public duties of organs of state will be drawn in an incremental and context-driven manner.

Thus, the Court's determination of the public interest will always be made on a consideration of the facts as a whole. There may be instances where there are potentially competing public interests, such as where a particular group stands to benefit, but there could be adverse consequences for other groups or the public more generally. Thus, all consequences of the processing (positive and negative) must be considered and given appropriate weight.[130]

125 Eg, in *Transnet Ltd t/a Metrorail & Others v Rail Commuters Action Group & Others* 2003 (6) SA 349 (SCA) para 17, per Howie P and Cloete JA, it was held to be sufficient that Metrorail provided transport services and the concept of 'public interest' did not impose any duties in relation to the safety or security of rail commuters.

126 *Transnet v Rail Commuters Action Group* (n 116) minority judgment of Streicher JA para 2.

127 Information Regulator of South Africa 'Guidance note on exemptions from the conditions for lawful processing of personal information in terms of section 37 and 38 of the Protection of Personal Information Act 4 of 2013' June 2021 para 4.2.3.3, https://justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Lawful Processing-202106.pdf (accessed 17 October 2021).

128 See eg *Asko Beleggings v Voorsitter van die Drankraad NO* 1997 (2) SA 57 (NC) 66H and 67E/F-F where the enquiry was whether the granting of a liquor store licence was in the interests of the residents of the town. Also see *Maharaj v Chairman, Liquor Board* 1997 (1) SA 273 (N).

129 Fittingly, the unanimous judgment of the Constitutional Court was penned by O'Regan J, the current designated COVID-19 judge. See *Rail Commuters Action Group & Others v Transnet Ltd t/a Metrorail & Others* 2005 (2) SA 359 (CC) para 85.

130 *Transnet v Rail Commuters Action Group* (n 116) 376B, approving *Clinical Centre (Pty) Ltd v Holdgates Motor Co (Pty) Ltd* 1948 (4) SA 480 (W) 489.

In a general sense, the COVID-19 monitoring and contact-tracing measures can be said to be in the public interest. That alone does not suffice. It must also be shown that the public interest in processing 'outweighs, to a *substantial degree*, any interference with the privacy of the data subject that could result …'[131] The concept of public interest thus is not an easy threshold to meet and will not exonerate responsible parties from incorporating protections for the privacy of personal information wherever this is reasonably possible.

As the capacity to collect and analyse digital data grows, sharp contests may be anticipated around the use of personal information by public and private entities alike. Similarly, contests will arise around access to information and freedom of expression, particularly media freedoms, where a distinction must be drawn been reporting in the public interest and reporting what is of mere interest to the public.[132] The concept of public interest may also shape the measures adopted to protect personal information in research.

## 5 Future COVID-19 research

The rapid development of testing kits and vaccines in the fight against COVID-19 resulted from an enormous collaborative effort within the health research community. Much of this research has necessarily relied upon the collection of personal information and POPIA contains a number of provisions that enable researchers to process personal information.

Processing special personal information such as health data is prohibited unless the data subject has consented to the collection of the data for the intended research purpose[133] or, in a research context,[134] where

> processing is for historical, statistical or research purposes to the extent that –
> (i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or
> (ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

131 POPIA secs 37(1)(a) & (b).

132 *Centre for Child Law v Media 24 Limited* 2020 (4) SA 319 (CC) para 100.

133 POPIA sec 27(1)(a) read with definition of consent under the Act.

134 POPIA sec 27(1)(d).

The requirements of section 27(1)(d) are less onerous than the requirements for a public interest exemption,[135] in that the researcher need only show that the effect of the processing is not disproportionately harmful to individual privacy, rather than the more stringent test of whether the public interest purpose of the processing 'substantially outweighs' the substantive value of the individual's privacy interest.

In addition, where another body has collected personal information (with the data subject's consent, or on another lawful basis) researchers can conduct secondary studies in reliance on the provisions of POPIA that such further processing is deemed compatible with the original purpose where it is for 'historical, statistical or research purposes' and 'will not be published in identifiable form'.[136]

Thaldar and Townsend rightly point out that if the original consent process were flawed, the secondary study would also be tainted.[137] This caution may apply to research using the proposed de-identified COVID-19 tracing database, if the data was not collected lawfully. On the analysis above, although it was lawful to collect the information without the data subject's consent, if the extent of the information collected about their location went beyond what was adequate and reasonably required for contact tracing, it should be deleted from the database and not made available to researchers.

It is only if the data was collected in full compliance with POPIA, and if it can be fully de-identified, that it will no longer be subject to POPIA. Nevertheless, even then, given the risk of re-identification, and the fact that the database contains special personal information about the health of individuals (their COVID-19 test results), as well as privacy-sensitive information about their location and movements, research ethics committees should pay careful attention to privacy and security safeguards in the proposed study.

In the case of other repositories of COVID-19 data, the source from which the data or specimens were collected and the justification for that collection will play a key role in determining whether further studies comply with POPIA or require fresh consent from the data subject. The Academy of Science of South Africa is presently facilitating the

135 POPIA sec 37(1) read with sec 37(2)(e) which expressly includes 'historical, statistical or research activity' in the meaning of the term 'public interest' under POPIA.

136 POPIA sec 15(3)(e).

137 DW Thaldar & BA Townsend 'Exempting health research from the consent provisions of POPIA' (2021) 24 *Potchefstroom Electronic Law Journal* 14.

development of a draft code of conduct for researchers, and it is to be hoped that the final code will adequately address this critical issue.

A code can only guide safeguards to comply with POPIA. It cannot amend the definition of consent, which POPIA requires to be informed, voluntary and *specific*.[138]

It follows that where the lawful justification processing was consent, then only narrow consent to a specified research purpose will suffice for processing special personal information such as health data. POPIA does not provide for broad consent, much less blanket consent to future as yet unspecified objectives. Tiered and broad consent may continue to be relied upon for ethical approval of the informed consent process required for all health research in terms of the National Department of Health's research ethics guidelines.[139] However, in such instances the research proposal would need to contain a different ground to justify processing any personal information collected, such as the public interest grounds set out in section 27 of POPIA.

## 6 Conclusion

It is vitally important that South Africa harness the power of data in an effective but responsible manner, both for effective governance and impactful evidence-based scientific research. POPIA supports these objectives, and highlights the importance of enabling the free flow of information, provided the personal information and privacy of individuals is protected.

Valuable lessons may be learned from the use of data by the government of South Africa in its response to the COVID-19 pandemic. The starting point for the analysis is that despite the importance of responding effectively and urgently to the pandemic, the right to privacy and the requirements for lawful processing under POPIA must be respected. In this regard the regulations creating the COVID-19 contract-tracing database implemented several important safeguards. Nevertheless, upon scrutiny, more could have been done to comply with the conditions for lawful processing. Before such data is released for research, any data collected outside the lawful bounds of the regulations, read with POPIA,

138 POPIA sec 1.

139 National Department of Health 'Ethics in Health Research Principles, Processes and Structures' 2015 para 3.3.6, https://www.ul.ac.za/research/application/downloads/DoH%202015%20Ethics%20in%20Health%20Research%20Guidelines.pdf (accessed 17 October 2021).

must be permanently deleted, and any other personal information must be de-identified to ensure that it is fully and irreversibly anonymised.

## References

Abdool Karim, SS 'The South African response to the pandemic' (2020) 382 *New England Journal of Medicine* e95

Bates, M 'Tracking disease: Digital epidemiology offers new promise in predicting outbreaks' (2017) 8 *IEEE pulse* 18

Bengtsson, L, Gaudart, J, Lu, X, Moore, S, Wetter, E, Sallah, K, Rebaudet, & Piarroux, R 'Using mobile phone data to predict the spatial spread of cholera' (2015) 5 *Scientific Reports* 1

Bradford, L, Aboy, M & Liddell K 'COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes' (2020) 7 *Journal of Law and the Biosciences* 34

De Montjoye, YA, Hidalgo, CA, Verleysen, M & Blondel, VD 'Unique in the crowd: The privacy bounds of human mobility' (2013) 3 *Scientific Reports* 1

Donnelly, D 'Privacy by (re)design: A comparative study of the protection of personal information in the mobile applications ecosystem under United States, European Union and South African law' PhD thesis, University of KwaZulu-Natal, 2020

Hagemeister, DT, Mpeli, MR & Shabangu, BE '"Please confirm your HIV-positive status by email to the following government address": Protection of "vulnerable employees" under COVID-19' (2020) 13 *South African Journal of Bioethics and Law* 91

Johnson, D 'Assessment of contact tracing options for South Africa' (October 2020) Research ICT Africa Cape Town, https://researchictafrica.net/wp/wp-content/uploads/2020/10/Contact-tracing-survey-report-David-Johnson-Oct2020.pdf (accessed 11 October 2021)

Marcello, I & Vayena, E 'On the responsible use of digital data to tackle the COVID-19 pandemic' (2020) 26 *Nature Medicine* 463

Mendelson, M & Madhi, S 'South Africa's coronavirus testing strategy is broken and not fit for purpose: It's time for a change' (2020) 110 *South African Medical Journal* 429

Rocher, L, Hendrickx, JM & De Montjoye, YA 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019) 10 *Nature Communications* 1

Singh, K 'Coronavirus: Authorities pull out all stops, high-level meeting planned with KZN school' 6 March 2020, https://www.news24.com/news24/SouthAfrica/News/coronavirus-authorities-pull-out-all-stops-high-level-meeting-planned-with-kzn-school-20200306 (accessed 11 October 2021)

Sun, N, Esom, K, Dhaliwal, M & Amon, JJ 'Human rights and digital health technologies' (2020) 22 *Health and Human Rights Journal* [special section 'Big Data, Technology, Artificial Intelligence and the Right to Health'] 21

Swales, L 'The Protection of Personal Information Act and data de-identification' (2021) 117 *South African Journal of Science* 1

Thaldar, DW & Townsend, BA 'Exempting health research from the consent provisions of POPIA' (2021) 24 *Potchefstroom Electronic Law Journal* 1

Viljoen, IM, De Villebois Castelyn, C, Pope, A, Botes, M & Pepper, MS 'Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa' (2020) 13 *South African Journal of Bioethics Law* 20

Wang, M 'China: Fighting COVID-19 with automated tyranny' *The Diplomat* 1 April 2020, https://thediplomat.com/2020/03/china-fighting-covid-19-with-automated-tyranny/ (accessed 18 October 2021)

Wu, JT, Leung, K & Leung, GM 'Nowcasting and forecasting the potential domestic and international spread of the 2019-nCoV outbreak originating in Wuhan, China: A modelling study' (2020) 395.1022 *The Lancet* 689