AFRICAN HUMAN RIGHTS LAW JOURNAL

To cite: W Lim 'Assessing the implications of digital contact tracing for COVID-19 for human rights and the rule of law in South Africa' (2020) 20 *African Human Rights Law Journal* 540-557
http://dx.doi.org/10.17159/1996-2096/2020/v20n2a8

Assessing the implications of digital contact tracing for COVID-19 for human rights and the rule of law in South Africa

*Woojin Lim**
Legal Researcher, International Justice and Human Rights Clinic, Peter A Allard School of Law, University of British Columbia
https://orcid.org/0000-0003-1931-6251

Summary: *The article argues that the establishment of centralised and aggregated databases and applications enabling mass digital surveillance, despite their public health merits in the containment of the COVID-19 pandemic, is likely to lead to the erosion of South Africa's constitutional human rights, including rights to equality, privacy, human dignity, as well as freedom of speech, association and movement, and security of the person. While derogation clauses have been invoked, thereby limiting International Covenant on Civil and Political Rights clauses and enabling the mass collection of location data only for contact tracing purposes under the Disaster Management Act, a sustained breach of these rights may pose an impending threat to the human rights framework in South Africa. Any proposed digital contact tracing technologies in their design, development and adoption must pass the firm legal muster and adhere to human rights prescripts relating to user-centric transparency and confidentiality, personal information, data privacy and protection that have recently been enacted through the latest development on Protection of Personal Information Act.*

* BA (Harvard); woojin_lim@protonmail.com. The views and errors expressed in this article are the author's own and do not purport to reflect the opinions of the International Justice and Human Rights Clinic at the University of British Columbia. I am grateful to the Journal for editorial guidance, and to Allison Stanger and Justin Julian Wong for their support in preparing this article.

Keywords: *digital contact tracing; COVID-19; Protection of Personal Information Act*

1 Introduction

The main objective of this article is to canvass the arguments around the human rights implications of digital COVID-19 contact tracing in South Africa. As evident in many countries across the globe, digital contact tracing has come with an expanded mass surveillance regime, the limitation of individual rights, and the stigma and shame associated with exposing the most private details of possible carriers. The second part of the article provides an overview of digital contact tracing in the age of COVID-19 in human rights terms, surveying the implementation of mobile phone-based contact tracing tools in South Africa since the Coronavirus outbreak. The latter half of the article explores a robust human rights advocacy framework and formulates legal regulatory safeguards that could be implemented in addition to currently existing data privacy laws to protect citizens from extended human rights violations. Legal and technical recommendations are embedded throughout the article.

The article also examines the compatibility of South Africa's proposed tracing database and associated applications with domestic and international privacy and data protection principles, including the Protection of Personal Information Act 4 of 2013 (POPIA) – which very recently became effective on 1 July 2020 – and the European Union (EU) General Data Protection Regulation (GDPR). Adopting a global comparative approach is key to replicating the successes and avoiding the failures that have arisen in other countries.

Crucially, the article finds that the establishment of centralised and aggregated databases and applications enabling mass digital surveillance – despite their public health merits in helping contain the COVID-19 pandemic – is likely to lead to the erosion of South Africa's constitutional human rights, including rights to equality, privacy, human dignity, as well as freedom of speech, association and movement, and security of the person. Any proposed digital contact tracing frameworks in their design, development and adoption must pass the legal muster and adhere to normative human rights prescripts relating to user-centric transparency and confidentiality, data privacy and protection, public accountability, non-discrimination and equality, concern and respect for the persons most affected in the process, whether in advocacy and monitoring or service provision.

2 Background on contact tracing in the age of COVID-19

Case and case-contact tracing has been frequented as a public health approach in government strategy to control the spread of the 2019 Coronavirus (COVID-19).[1] Employed previously to contain the 2014 Ebola virus outbreaks in Africa, the main purpose of this practice is to rapidly identify secondary cases caused by the first probable or confirmed cases, to track possible routes of infection, mitigate the flaws of detection based only on symptoms, and break the chain of onward transmission.[2] The key steps of contact tracing involves contact identification, listing and follow-up, in an attempt to 'effectively measure the actual number of infected members of the population'.[3] Compelling public health reasons – namely, that COVID-19 is transmitted via respiratory droplets and direct contact with infected carriers[4] – pave the way for exit strategies for a phased lifting of lockdown regulations that require contact tracing in synergy with other measures such as rapid testing and social distancing.[5]

Conventionally, contact tracing has been performed in a manual setting, where a public health worker would engage in a phone conversation with each diagnosed carrier to retrace preceding weeks of the carriers' lives. Exercising careful discretion, the health worker would afterwards identify those in close contact with the carriers and notify those close contacts to isolate and seek testing.[6] In South Africa approximately 20 000 people have been trained to assist with manual contact tracing.[7] At this stage of the COVID-19 outbreak, however, manual contact tracing has many setbacks due to its labour-intensive processes and the limited testing kits available. Manual contact tracing may also be fraught with memory errors.

1 Johns Hopkins University 'Coronavirus Resource Center', www.coronavirus.jhu.edu/ (accessed 1 October 2020).
2 WHO 'Contact tracing during an outbreak of Ebola virus disease' September 2014, www.who.int/csr/resources/publications/ebola/contact-tracing-during-outbreak-of-ebola.pdf (accessed 1 October 2020).
3 WHO 'Contact tracing in the context of COVID-19' 10 May 2020, www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19 (accessed 1 October 2020).
4 WHO 'Modes of transmission of virus causing COVID-19: implications for IPC precaution recommendations' 29 March 2020, www.who.int/news-room/commentaries/detail/modes-of-transmission-of-virus-causing-covid-19-implications-for-ipc-precaution-recommendations (accessed 1 October 2020).
5 UN 'Technical Guidance on contact tracing for COVID-19 in the WHO African region' April 2020, www.afro.who.int/publications/technical-guidance-contact-tracing-covid-19-world-health-organization-who-african (accessed 1 October 2020).
6 As above.
7 IM Viljoen et al 'Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa' (2020) 13 *South African Journal of Bioethics and Law* 15.

New and emerging methods of contact tracing have included mobile phone applications or Bluetooth networks which could expedite an existing manual contact tracing operation and make it more accurate by finding close contacts that were unknown to or forgotten by carriers; additionally, digital applications can anonymously and automatically alert potentially exposed users.[8] One such example is Google and Apple's decentralised approach, which puts to the fore in its design principles of user privacy and security. Proponents of (at least certain forms of) digital contact tracing argue that technological automation can at least supplement the work of manually identifying those who have been exposed to COVID-19.[9] Digital surveillance has played an essential role in containing the COVID-19 pandemic in China, Singapore, Israel and South Korea, among others.[10]

Databases gathered from contact tracing investigations have been collated and analysed to view larger patterns, including transmission sites, attack rates, and the effectiveness of mitigation measures, contributing to a better understanding of the epidemiology of COVID-19 and assisting with policy formulation. Each country has been advised to adapt their rapid response based on the local epidemiological situation and its available resources.[11]

2.1 Deployment of digital contact tracing tools for COVID-19 in South Africa

Upon the identification of the first cases in South Africa, President Cyril Ramaphosa swiftly declared a national state of disaster on 15 March 2020, invoking section 27(1)(b) of the Disaster Management Act 57 of 2002 (DMA) and declaring contact tracing

8 M Ienca & E Vayena 'On the responsible use of digital data to tackle the COVID-19 pandemic' (2020) 26 *Natural Medicine* 463-464. The article shows the effectiveness of mobile phone data and big data analytics in predicting the spatial spread of cholera during the 2010 Haiti cholera epidemic and during the 2014-2016 Western African Ebola crisis; See, eg, Apple and Google 'Privacy-preserving contact tracing' (2020), https://covid19.apple.com/contacttracing (accessed 1 October 2020).

9 See J Valentino-DeVries et al 'A scramble for virus apps that do no harm' *The New York Times* 3 June 2020, www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html (accessed 1 October 2020).

10 L Bradford, M Aboy & KL Liddell 'COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes' (2020) 7 *Journal of Law and the Biosciences* 1; J Valentino-DeVries 'Translating a surveillance tool into a virus tracker for democracies' *The New York Times* 19 March 2020, www.nytimes.com/2020/03/19/us/coronavirus-location-tracking.html (accessed 1 October 2020).

11 European Centre for Disease Prevention and Control 'Contact tracing: Public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – Second update' 8 April 2020.

as 'crucial and non-negotiable'.[12] The government shortly thereafter, on 18 March 2020, published amended regulations for contact tracing in the Government Gazette.[13]

South Africa has since joined several governments in passing regulations that allow for the identification of infection hotspots using technology, surveillance data, epidemiological mapping, as well as the collection and storage of data from mobile companies. On 26 March 2020 the Minister of Communications and Digital Technologies directed the operations of the electronic communications sector as essential services to combat the spread of COVID-19 in South Africa, pursuant to regulation 10(8) of the Regulations issued in relation to section 27(2) of the DMA. Part of these directions includes 'individual track and trace' under sections 8(1) and 8(2) according to which the internet and digital sectors must provide location-based services to 'track and trace individuals that have been infected and such other persons that may have been in direct contact with such infected persons. A database may be correlated with other sources from government and private sector.'[14]

Health data safeguards under the Protection of Personal Information Act 4 of 2013 (POPIA) – which has been a work in progress since it was designated for implementation by the South African Law Reform Commission in 2005 – were due to take effect on 1 April 2020, but POPIA has been postponed in light of the COVID-19 outbreak.[15] Although only certain provisions of POPIA were legally binding in the early stages of COVID-19, the remaining provisions of POPIA have since become effective, starting on 1 July 2020, with provisions relating to the oversight of the access to information commencing on 30 June 2021.[16] Given POPIA's large-

12 C Ramaphosa 'South Africa's response to Coronavirus COVID-19 pandemic' 13 May 2020. In the speech, South Africa's President Ramaphosa enlists a number of Coronavirus prevention measures two months after the declaration of a national state of disaster as a result of COVID-19.

13 Department of Cooperative Governance and Traditional Affairs 'Declaration of a national state of disaster. Government Notice 313 in Government Gazette 43096' 15 March 2020. See also South Africa's Coronavirus guidelines, including core lockdown regulations, directions, disaster management guidelines and notices, and the Disaster Management Act amendments.

14 See *Government Gazette* 'Electronic communications, postal and broadcasting directions issued under Regulation 10(8) of the Disaster Management Act, 2002 (Act No 57 of 2002)' 26 March 2020.

15 Protection of Personal Information Act (POPIA) 4 of 2013, 26 November 2013. Sec 26 of POPIA provides restraints on the processing of special personal information and requires the consent of the data subject. This clause would remain in place unless processing is necessary for the exercising of a right or obligation in law.

16 'South Africa's Protection of Personal Information Act, 2013, goes into effect July 1' *The National Law Review* 29 June 2020, www.natlawreview.com/article/south-africa-s-protection-personal-information-act-2013-goes-effect-july-1 (accessed 1 October 2020); N Bowan 'After 7-year wait, South Africa's Data

scale impact on privacy rights, it is required that all processing of personal information must conform with its set out provisions within one year after its commencement, that is, a 12-month grace period that ends on 1 July 2021. In the meantime, POPIA's implications for digital contact tracing yet remain in limbo, which gives all the more reason to ensure that the handling of personal data in digital contact tracing complies with these new regulations. The situation is very much still developing, as POPIA has recently been enacted in the midst of the 12-month grace period for compliance. In view of a roadmap and concrete implementation plans, organisations subject to POPIA and GDPR regulations must be flexibly willing to adjust their operational capabilities and governance structures. Given that there is no silver bullet solution to data protection compliance when it comes to GDPR or POPIA, it is important to retain flexibility when assessing and identifying mitigating controls.

In addition, section 14 of the Bill of Rights (Chapter 2 of the Constitution), or the common law, both recognise and protect the right to privacy.[17] Given that privacy laws in South Africa are in their early stages of enshrinement, residual concerns remain about how personal information is being handled and protected during the outbreak.

Building on earlier developments, on 2 April 2020 South Africa established the COVID-19 tracing database, a new electronic database collected by electronic communication service providers (ECSPs) licensed under the Electronic Communications Act 36 of 2005. At the written request of the Director-General of Health, ECSPs must provide the location or movements of any person known or reasonably suspected to have contracted COVID-19. The tracing database includes the collection of names, identity and passport numbers, cellphone numbers, and test results for those tested for COVID-19 and their known or suspected contacts. The purpose of this database is 'to enable the tracing of persons who are known or

---

Protection Act enters into force' IAPP, https://iapp.org/news/a/after-a-7-year-wait-south-africas-data-protection-act-enters-into-force/ (accessed 1 October 2020). POPIA's secs 2 to 38, secs 55 to 109, sec 111 and sec 114 have entered into full force. These new additions to POPIA provide eight essential conditions for lawful processing of data: (i) accountability; (ii) processing limitation; (iii) purpose specification; (iv) further processing limitation; (v) information quality; (vi) openness; (vii) security safeguards; and (viii) data subject participation.

17 See Constitution of the Republic of South Africa, 1996, amended on 11 October 1996 by the Constitutional Assembly. The final version of the South African Bill of Rights states that its provisions bind the judiciary (sec 8(1)), natural and juristic persons (sec 8(2)) and oblige a court 'in applying the provisions of the Bill of Rights to natural and juristic persons' to develop the common law 'to the extent that legislation does not give effect to that right' (sec 8(3)).

reasonably suspected to have come into contact with any person known or reasonably suspected to have contracted COVID-19'.[18]

The South African government in partnership with the University of Cape Town has developed and launched a smartphone contact tracing application, COVi-ID, which tracks individuals who have come into contact with others who have tested positive. The application lets users prove their COVID-19 status through QR codes which retrieve the user's health status. On 2 May 2020 the Department of Health also launched COVIDConnect, a WhatsApp and SMS-based symptom reporting process, which works on any mobile phone.[19]

Most recently, South Africa's health department launched Covid Alert SA, a mobile phone application that draws from Apple and Google's Bluetooth-based exposure notification Application Programming Interface (API). The application uses Bluetooth to pick other users who are in the same radius and lets each user build an 'encounter history' of those they have encountered.[20]

These changes have resulted in the creation of a personal electronic contact tracing database in which carriers and individuals suspected of having been infected with COVID-19 or coming into contact with infected persons could be collected. Mobile operators have been obligated to provide mobile data by using digital surveillance technologies to manage the COVID-19 outbreak.[21] The new COVID-19 regulations have authorised the Director-General of Health to issue and oversee tracking orders. Significantly, the legal regulations establishing the use of individualised data for contact tracing goes beyond the initial reported intention of the Council for Scientific and Industry Research (CSIR), which is to aggregate location data for analytical purposes and to provide evidence for rational crisis response and policy making.

18 J Klaaren et al 'South Africa's COVID-19 tracing database: Risks and rewards of which doctors should be aware' (2020) 110 *South African Medical Journal* 617-620.

19 Z Mkhize 'Reduction in the isolation period for patients with confirmed COVID-19 infection' Department of Health, Republic of South Africa 17 July 2020, www.sacoronavirus.co.za/2020/07/17/reduction-in-the-isolation-period-for-patients-with-confirmed-COVID-19-infection (accessed 1 October 2020); R Lake et al 'Contact tracing apps in South Africa' Norton Rose Fulbright 11 May 2020.

20 'Health launches COVID-19 contact tracing app' *SA News* 2 September 2020, https://www.sanews.gov.za/south-africa/health-launches-covid-19-contact-tracing-app (accessed 1 October 2020). The application has proven legally sound through consultation with Justice Catherine O'Regan, the COVID-19 designated judge.

21 W Strachan & T Cohen 'South Africa: Coronavirus (COVID-19): Obligations and roles of the electronic communications sector published' ENSight: Technology, Media, Telecommunications 27 March 2020.

2.2 Technical challenges, implementation concerns and scope-based limitations

Given the fact that only around one-third of the country's population regularly use smartphones,[22] the larger remainder of the population is vulnerable to lack of access, contributing to low penetration rates and limited application while deepening socio-economic divides. Furthermore, as South Africa relies on the triangulation of cell tower metadata supplied by ECSPs, this is problematic both for rural areas that have few towers and urban areas where buildings scatter signals.[23] Oxford researchers predict that while a 60 per cent take-up of digital contact tracing would work best, a lower rate of engagement might still contribute to a reduction in cases.[24] Given these limitations of viable options, effectiveness and accuracy must be improved so as to suture inequalities.

That said, even with sufficient scientific evidence that contact tracing applications contribute to securing the rights to life and health, policy makers must not be lured by the false pretense that technology will allow them to sidestep difficult ethical and human rights dilemmas. Policy makers must be mindful that privacy-preserving protocols may overlook those who cannot afford reliable mobile connections for reasons of age, disability or poverty.[25]

3 Human rights framework

The COVID-19 outbreak has brought debates concerning human rights to the centre of public discourse. The proliferation of unprecedented technologies – including geolocation, biometric data, facial recognition, artificial intelligence, big data – have

22 Estimates by Statista show that around 20 to 22 million people in South Africa regularly use a smartphone, www.statista.com/statistics/488376/forecast-of-smartphone-users-in-south-africa/ (accessed 1 October 2020); S Stolton 'EU data watchdog very worried by Hungary's GDPR suspension' *Euractiv* 18 May 2020, www.euractiv.com/section/data-protection/news/eu-data-watchdog-very-worried-by-hungarys-gdpr-suspension/ (accessed 1 October 2020).

23 MS Pepper & M Botes 'Balancing privacy with public health: How well is South Africa doing?' *The Conversation* 24 June 2020, www.theconversation.com/balancing-privacy-with-public-health-how-well-is-south-africa-doing-140759 (accessed 1 October 2020).

24 University of Oxford Research 'Digital contact tracing can slow or even stop Coronavirus transmission and ease us out of lockdown' 16 April 2020, www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown (accessed 1 October 2020).

25 A Toh & D Brown 'How digital contact tracing for COVID-19 could worsen inequality' *Just Security* 4 June 2020, www.justsecurity.org/70451/how-digital-contact-tracing-for-covid-19-could-worsen-inequality/ (accessed 1 October 2020).

offered significant potential to track impacted populations, enforce COVID-19 self-isolation rules in South Africa, and meet fundamental human rights principles concerning the rights to life and health.[26] International human rights law guarantees every person the right to the highest attainable standard of health and recognises that in the context of serious public health threats to the life of the nation, restrictions on some rights may be justified. All the while, these measures, if taken beyond the scope of necessity, may incur enormous trade-offs on human rights and constitutional freedoms.[27]

While the right to privacy and mobility clearly is being limited in light of exceptional public health circumstances, including the right to health, many of the deployed digital technologies have been excessively data-intensive and prone to abuse by corporate and government entities.[28] In addition, the process of imposing emergency COVID-19 regulations have often overlooked usual procedures of democratic deliberation and the consultation of persons concerned. Thus, the digital contact tracing efforts must be monitored and limited by the rule of law, fulfilling the conditions set by human rights conventions. The legal and medical community must be aware of the vast mass surveillance regime and its looming risk to human rights. Neither the right to privacy nor the right to health and the freedom of science bears an absolute precedence over the other. Hence, these rights and freedoms must be carefully and responsibly balanced, broaching an outcome that respects the essence of both sides.

The mission creep of large-scale digital surveillance paves the way for corporate entities or the government to potentially abuse personal information and further alienate communities that have already

26 Under the International Covenant on Economic, Social and Cultural Rights (ICESCR), which South Africa ratified in January 2015, everyone has the right to 'the highest attainable standard of physical and mental health'. Effective steps must be taken for the 'prevention, treatment and control of epidemic, endemic, occupational and other diseases'. Human Rights Watch 'Human rights dimensions of COVID-19 response' 19 March 2020, www.hrw.org/news/2020/03/19/human-rights-dimensions-COVID-19-response (accessed 1 October 2020); L Forman 'The evolution of the right to health in the shadow of COVID-19' (2020) 22 *Health and Human Rights Journal* 375.

27 International Bar Association 'Digital contact tracing for the COVID-19 epidemic: A business and human rights perspective' (2020), www.business-humanrights.org/sites/default/files/documents/LPRU-Digital-contact-tracing-COVID-19-June-2020.pdf (accessed 1 October 2020).

28 In China a lack of transparency has caused an environment of fear and bewilderment amid suspicions that monitoring tools have outlasted their original purpose. Neither the contact tracing company nor Chinese officials have been transparent about how the system classifies individuals, and users suspect that the application carries the risk of reporting personal data to the police. P Mozur, R Zhong & A Krolik 'In Coronavirus fight, China gives citizens a color code, with red flags' 1 March 2020, www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html (accessed 1 October 2020).

suffered longstanding human rights violations.[29] Such tracking, if extended by bad actors beyond the immediate COVID-19 response, can upscale invasive mass surveillance practices, limit individual rights and freedoms, discriminate against specific populations or marginalised groups, and expose stigmatising personal details about diagnosed carriers of the virus.[30] Human rights limitations occurring outside of the standard democratic process must be minimal and treated as exceptions to the norm, subject to careful scrutiny and justification.[31]

Current built-in safeguards against the outlasting of data privacy risks in South Africa (as of 7 August 2020) include a strict duration requirement and reporting requirements to a COVID-19 designated judge. The amended disaster management regulations created shortly thereafter, on 2 April 2020, limit the scope of the collection of mobile data only for the purposes of contact tracing, accessible specifically by the Director-General of the Department of Health. The Minister of Justice and Correctional Services has appointed Justice Kate O'Regan, a retired judge of the Constitutional Court, to serve as the COVID-19 designated judge.[32] Extended safeguards must be instituted to prevent the normalisation of data privacy infringements.

The United Nations (UN) has acknowledged that human rights provide a critical framework for the COVID-19 outbreak response because '[human rights] put people at the centre and produce better outcomes'.[33] Observing COVID-19 digital contact tracing tools through a human rights lens ensures a focus on how to preserve human dignity for those who are most vulnerable while ensuring that the design and deployment of digital contact tracing applications are tested against the principles of necessity, proportionality and legality

29 See YN Harari 'The world after Coronavirus' 19 March 2020, www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (accessed 1 October 2020). One of two particularly important choices that he lists is the choice between totalitarian surveillance and citizen empowerment. Harari writes: 'One of the problems we face in working out where we stand on surveillance is that none of us know exactly how we are being surveilled, and what the coming years might bring.'

30 Diagnosed carriers, when identified publicly, have been subjected to public stigmatisation and social repercussions. In South Korea, eg, data sent out by the South Korean government to inform residents about the GPS movements of diagnosed carriers has caused online witch hunts, creating an atmosphere of fear. See MS Kim 'South Korea is watching quarantined citizens with a smartphone app' MIT Technology Review 6 March 2020, www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/ (accessed 1 October 2020); 'Coronavirus privacy: Are South Korea's alerts too revealing?' *BBC News* 5 March 2020, www.bbc.com/news/world-asia-51733145 (accessed 1 October 2020).

31 See Viljoen et al (n 7).

32 Government of South Africa 'Minister Ronald Lamola appoints Justice Kate O'Regan as Coronavirus COVID-19 designate judge' 3 April 2020.

33 UN 'COVID-19 and human rights: We are all in this together' (2020).

as required by South Africa's Constitution and its undertakings in international law.[34] Other international watchdogs and human rights organisations have followed suit by drafting statements and guidelines for ethical data management during the outbreak.[35]

3.1 Limitation and derogation of international human rights under an extended state of emergency

The right to privacy, enshrined in article 17 of the International Covenant on Civil and Political Rights (ICCPR), is a qualified right that may be restrained under certain conditions.[36] According to article 4 of the ICCPR, during a state of public emergency which threatens the life of the nation, state parties can exceptionally and temporarily curtail certain rights recognised by ICCPR. The 1984 Siracusa Principles, building on the applicable derogation clause in ICCPR, call for the authoritative limitation of certain rights in response 'to a pressing public or social need' such as public health.[37]

In order for a state to derogate under these principles, the following six conditions must be met: (i) the existence of a public emergency threatening the life of the nation; (ii) the measures adopted must be strictly necessary by the exigencies of the situation; (iii) the measures must not be discriminatory; (iv) derogating measures are only permissible if not inconsistent with other international obligations; (v) it cannot be justified for non-derogable rights; and

34 M Hunter 'Cops and call records: Policing and metadata privacy in South Africa' Media Policy and Democracy Project, March 2020.

35 Human Rights Watch 'Joint civil society statement: State's use of digital surveillance technologies to fight pandemic must respect human rights' 2 April 2020, www.hrw.org/news/2020/04/02/joint-civil-society-statementstates-use-digital-surveillance-technologies-fight (accessed 1 October 2020); United Nations Office of the High Commissioner on Human Rights 'COVID-19: States should not abuse emergency measures to suppress human rights' (2020); Human Rights Watch 'Human rights dimensions of COVID-19 response' 19 March 2020, www.hrw.org/news/2020/03/19/humanrights-dimensions-COVID-19-response (accessed 1 October 2020); S Zarifi & K Powers 'Human rights in the time of COVID-19: Front and centre' International Commission of Jurists 6 April 2020, www.icj.org/human-rights-in-the-time-of-covid-19-front-and-centre/ (accessed 1 October 2020).

36 See International Covenant on Civil and Political Rights, adopted by General Assembly Resolution 2200A (XXI) of 16 December 1966, 999 UNTS171 (ICCPR). Non-derogable rights listed under sec 2 of art 4 include the right to life (art 6); prohibition of torture, cruel, inhuman and degrading treatment (art 7); prohibition of medical or scientific experimentation without consent (art 7); prohibition of slavery, slave trade and servitude (art 8); prohibition of imprisonment because of inability to fulfil contractual obligation (art 11); principle of legality in criminal law (art 15); recognition everywhere as a person before the law (art 16); freedom of thought, conscience and religion (art 18).

37 Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights April 1985; A Ghose & DD Sokol 'Unlocking platform technology to combat health pandemics' (2020) *Yale Journal on Regulation* 3.

(vi) these derogations also require that states formally declare a state of emergency and, in the case of ICCPR, formally notify the UN Secretary-General.[38]

In addition, the Siracusa Principles require that the essence of the right must not be undermined; the legal rules limiting the exercise of human rights must pursue a legitimate aim; must be prescribed by a 'clear and accessible' law; must 'not be arbitrary or unreasonable'; and that 'adequate safeguards and effective remedies' be provided against the imposition of abusive limitations. The measures must also be purpose-limited to the specific aim of 'preventing disease or injury or providing care for the sick and injured'.[39]

On 30 April 2020, the UN Human Rights Committee issued the 'Statement on derogations from the Covenant in connection with the COVID-19 pandemic' in which the Committee highlighted that states have resorted to emergency measures by severely restricting fundamental rights and freedoms. In contrast, the African Charter on Human and Peoples' Rights (African Charter) does not mention or contain any derogation provisions, although state parties may derogate from certain rights in times of emergency.[40]

The South African Bill of Rights, including section 14 on privacy, also contains a derogation clause in section 36: These fundamental rights may only be limited in terms of law of general application, that is, 'to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom'.[41] Relevant factors to be considered for limitation include the nature of the right, the purpose and extent of limitation, how the limitation relates to its purpose, and whether there are less restrictive alternative means to achieve the purpose.

3.2 Transparency principles and international guidelines

A number of other important yet overlooked principles that were absent from South Africa's COVID-19 disaster regulations included principles of transparency and data security. POPIA's older cousin in Europe could be considered: the OECD Privacy Guidelines and

38 UN Commission on Human Rights 'The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' 28 September 1984, E/CN.4/1985/4, https://www.refworld.org/docid/4672bc122.html (accessed 1 October 2020).
39 As above.
40 Max Planck Encyclopedia of Public International Law *African Charter on Human and Peoples' Rights* (1981).
41 South African Constitution Ch2: Bill of Rights.

the European Commission's (EU) General Data Protection Regulation (GDPR), which came into effect on 25 May 2018 (although GDPR was formally adopted in May 2016).[42] GDPR is hailed as the aspirational global legislative standard for protecting the rights of individuals whose personal information enters the digital world. GDPR has been cited by legal analysts as one of the main reasons for the delay of POPIA, which gave South African privacy regulators time to develop operational capabilities.[43] POPIA and GDPR currently align and overlap in most areas, which means that compliance with GDPR should result in nearly full compliance with POPIA.

GDPR's comprehensive fundamental rights include the right to transparency and information (that is, organisations must in a clear, fair, and transparent manner provide data subjects with information about who has access to their personal data, for what purpose it will be used, who the recipients will be, and the period for which the information will be stored); the right to be forgotten (that is, individuals may request that their personal information be released without undue delay subject to the grounds that the usage of the personal data is no longer relevant for the original purpose for which it was collected and processed); the right to restrict data processing (that is, individuals may contest the lawfulness and accuracy of the information); and the right to access (that is, individuals should be informed whenever an organisation processes their information within a reasonable time period, receive a copy of their information, and be afforded the opportunity to lodge a complaint against undue collection and processing).[44]

On 21 April 2020 the European Data Protection Board (EDPB), which oversees consistent compliance with GDPR, issued legal guidelines on the processing of health data for scientific research purposes in the context of the COVID-19 outbreak.[45] The document

42 The GDPR does not have general effect in South Africa as it is not a local law of the country, but certain parties that process information in South Africa might still need to comply with GDPR due to its 'extraterritorial application'. See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 23 September 1980 C(80)58/FINAL 1980) (OECD Guidelines). This was revised as OECD Privacy Framework in 2013, www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed 1 October 2020).

43 DLA Piper 'Data protection laws of the world: South Africa vs United Kingdom' 29 September 2020.

44 B McKenzie 'General Data Protection Regulation (GDPR) in Africa: So what?' 4 July 2019, www.bakermckenzie.com/en/insight/publications/2019/05/general-data-protection-regulation (accessed 1 October 2020).

45 European Data Protection Board 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' adopted 21 April 2020; European Data Protection Board 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' adopted 21 April 2020.

notes that GDPR data protection rules themselves do not hinder the public health effort in the fight against the COVID-19 outbreak.[46] The GDPR, as a broad piece of legislation, foresees the handling of personal data for the sole purpose of scientific research in compliance with the fundamental rights to privacy and personal data protection.[47]

3.3 Personal data protection in South Africa

The GDPR provides South Africa with an overarching yardstick by which to measure its own respective national privacy laws.[48] By way of comparison, the delay of POPIA has left South Africa exposed to a number of human rights violations since the COVID-19 outbreak.[49] In view of the fact that POPIA is in its early stages as binding law, it is legally permissible to collect, store and use the aforementioned personal data without the subject's consent in line with the Disaster Management Act.[50] Furthermore, Regulation 15(2) of the Regulations Relating to the Surveillance and the Control of Notifiable Medical Conditions, issued in terms of the National Health Act 61 of 2003,[51] allows the head of a provincial health department to apply for an appropriate court order if a person who is a confirmed carrier refuses to be tested or subjected to a medical examination. The information

46 European Data Protection Board 'Statement on the processing of personal data in the context of the COVID-19 outbreak' 20 March 2020, https://edpb.europa.eu/our-work-tools/our-documents/outros/statement-processing-personal-data-context-COVID-19-outbreak_en (accessed 1 October 2020).

47 All processing of personal health data must be in line with principles relating to the proceedings set out in art 5 of GDPR. See arts 6 and 9 of GDPR for legal grounds and derogations.

48 See J Burchell 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 *Electronic Journal of Comparative Law*; for earlier guidelines on information privacy, see *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC) where the Constitutional Court listed general guidelines that govern data protection, including whether the information was obtained in an intrusive manner, whether the information contains intimate aspects of the subject's personal life, and whether it was disseminated to the press or general public from whom the subject 'could reasonably expect such information would be withheld'.

49 Secs 19 to 22 of POPIA provide for various security measures on 'integrity and confidentiality of personal information, the processing of information, security measures to be taken and the notification requirements in case of any security compromises'.

50 Regarding organised criminal activity, cellular phone data can be accessed under secs 7(1) and (2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), and under sec 205 of the Criminal Procedure Act 51 of 1977. However, provided the circumstances of civilians, these two laws do not seem relevant here. See Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 and Criminal Civil Procedure Act 51 of 1977.

51 National Department of Health of South Africa 'Regulations relating to the surveillance and the control of notifiable conditions' *Government Gazette* 40945:604 30 June 2017, www.nicd.ac.za/wp-content/uploads/2017/12/41330_15-12_Health-compressed.pdf (accessed 1 October 2020).

required by the contact tracing database may be lawfully obtained without the consent of the infected or supposedly infected individual.

3.4 Impact on marginalised groups and victims of domestic abuse

In a joint white paper, domestic abuse and violence against women and girls (VAWG), experts were concerned that digital contact tracing could become a 'tool for abuse' in the case that contact and location details of survivors could be leaked to perpetrators.[52] In addition, domestic violence and child abuse has spiked in number, frequency and intensity during COVID-19 lockdowns.[53] As a signatory of the UN Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), South Africa must take all adequate steps to ensure that information obtained from digital contact tracing does not get leaked to perpetrators of violence and domestic abuse.[54] Digital contact tracers must be mindful of the diverse array of impacts that their technology could have on marginalised and vulnerable groups, whereas digital contact tracing applications should be designed with the aim of empowering rather than stigmatising and repressing individuals.

4 Legal recommendations

The framework of how digital contact tracing will operate should be set out in primary legislation. Providing human rights instruments as safeguards is indispensable for increased uptake, social acceptability and public trust, causing people to be more likely to follow public health advice and recommendations.[55] The government must invoke safeguards to ensure that such personal information is collected, stored, assessed, distributed and processed in accordance with human rights principles and thereon balances the imposed

52 'COVID-19 contact tracing apps could be turned into tools for domestic abuse' *Forbes* 22 June 2020, www.forbesafrica.com/technology/2020/06/22/warning-COVID-19-contact-tracing-apps-could-be-turned-into-tools-for-domestic-abuse/ (accessed 1 October 2020).

53 Oxford Human Rights Hub 'COVID-19 and domestic violence in South Africa' 28 April 2020, ohrh.law.ox.ac.uk/COVID-19-and-domestic-violence-in-south-africa/ (accessed 1 October 2020).

54 United Nations 'Convention on the Elimination of All Forms of Discrimination against Women' 18 December 1979; T Peacock et al 'The law during a state of disaster and human rights risks' C19 People's Coalition.

55 Scottish Human Rights Commission 'COVID-19: Human rights implications of digital contact tracing technology' 18 May 2020; PR Ward 'Improving access to, use of, and outcomes from public health programs: The importance of building and maintaining trust with patients/clients' (2017) 5 *Public Health* 22.

COVID-19 restrictions fairly and justifiably. The implementation of these principles must constantly be verified and updated.

The drafting of primary legislation – or at least a guidance note – should address the following issues, namely, the justification of data collection; narrow limitations around who will have access to the database (non-disclosure agreements, access logs, and strict access role distribution); a guarantee of secure storage and deletion of sensitive data when no longer needed (storage timelines); transparent measures that inform data subjects about the type of information collected; robust review and independent oversight mechanisms; and confirmation of an individual's ability to exercise other fundamental rights and freedoms once lockdown measures are eased.[56] Part of this framework would include granting the implementation of the relevant sections of POPIA about the processing of personal information in terms of aforementioned GDPR provisions, and using this opportunity to leverage the implementation of stricter data privacy protections. Instead of invoking narrow sector-focused rules, which may involve bridging difficulties in the middle of a national emergency, the comprehensive principle-based approach of international data protection standards can provide expansive scope and flexibility.[57]

Where possible, digital application designers should attempt to build pseudonymisation, decentralisation and encryption protections into the data collection processes themselves, for instance, by avoiding centralised databases, not identifying proximity or interaction data, and adopting Bluetooth exposure notification systems and QR code scanning.[58] Concomitant with these human rights principles, professional technical expertise must be hired to ensure the adequate enforcement of security and secrecy. Knowledge sharing of best practices among cross-sectorial interventions should be encouraged in order to maintain responsible data collection and processing standards.[59] Any restriction of the rights of monitored individuals must be applied only insofar as it is strictly necessary.

Independent oversight of all measures introduced in response to the COVID-19 outbreak is needed beyond the appointment of

56 Ienca & Vayena (n 8) 463-465; Bradford et al (n 10).
57 R Raskar et al 'Apps gone rogue: Maintaining personal privacy in an epidemic' PrivateKit: MIT 19 March 2020. MIT's Private Kit: Safe Paths is a privacy-first, open-source contact tracing technology that works with a 'pull model' where 'users can download encrypted location information about carriers … self-determine their likely exposure to COVID-19 and coordinate their response with their doctor using their symptoms and personal health history'.
58 Ada Lovelace Institute 'Exit through the App Store?' 20 April 2020.
59 Klaaren et al (n 18) 617-620.

Justice Kate O'Regan, supplemented with constant comparisons of national and international privacy laws using GDPR as a baseline. The overseeing judge should also have the right to inspect the databases and look at the security of those databases. More oversight is required around the use, effectiveness, inspection and privacy provisions of any contact tracing applications and databases. Policy makers and application designers should be held accountable for extended encroachment on human rights.

The principles of equality, dignity and non-discrimination are the bedrock of human rights law, recognised as norms in both the domestic and international framework. South Africa must interpret and apply these principles consistently in its laws and regulations. The collection, retention and deletion of data should in particular consider the circumstances of the most vulnerable and disadvantaged groups impacted by COVID-19 contact tracing applications – those groups that are less likely to access a contact tracing application for a number of reasons including, but not limited to, disability, poverty and age. To help those suffering under domestic violence, helpline services must be expanded, while hotel rooms for abuse victims and makeshift counselling centres should be provided in accordance with CEDAW and other legal structures that remain operational during the lockdown. Adopting interoperable frameworks, guided by EDPB's response to the use of digital contact tracing applications during the pandemic, can ensure compliance with international legal standards for human rights protections.

5 Conclusion

The COVID-19 outbreak has paved the way for the introduction of a number of rapid response restrictions of individual freedoms, adversely impacting carriers' enjoyment of their human rights in countries all over the world. The use of digital contact tracing is an essential piece of a wider strategy to combat the virus. However, it is important to secure limits around the governance of data and technology by setting these out clearly in law, ensuring that any mass data collection is necessary and proportionate, time-bound and limited in duration, respectful of human dignity, non-discriminatory in application, and subject to ongoing review and public scrutiny. Transparent public communication about digital contact tracing protocols for the common good should be issued in conjunction with independent oversight. More than ever, human rights practitioners, medical professionals and contact tracers from all walks must be prepared to move with force in defending human rights standards and protect the communities that are most

vulnerable to infection and rights infringement. Following South Africa's implementation of the relevant sections of POPIA and the National Department of Health's launch of the COVID-19 Alert SA exposure notification framework, international human rights law must be carefully observed and applied through and by all relevant actors, strengthening the interpretation and application of human rights norms, especially that of privacy. African states, including South Africa, must continue to carefully monitor new forms of digital contact tracing and stay updated on the technical architecture so as to circumvent a serious threat to human rights globally.