

## MEDICINE AND THE LAW

# South Africa's COVID-19 Tracing Database: Risks and rewards of which doctors should be aware

J Klaaren,<sup>1,2</sup> BA, MA, JD, LLB, PhD; K Breckenridge,<sup>2</sup> BA, BA Hons, PhD; F Cachalia,<sup>2</sup> BA, BA Hons, LLB, LLM, HDip;  
S Fonn,<sup>3</sup> DOH, MB BCh, Dip Epi, PhD, FFCH (SA); M Veller,<sup>4</sup> MB BCh, MMed, FCS (SA)

<sup>1</sup> School of Law, University of the Witwatersrand, Johannesburg, South Africa

<sup>2</sup> Wits Institute for Social and Economic Research, University of the Witwatersrand, Johannesburg, South Africa

<sup>3</sup> School of Public Health, University of the Witwatersrand, Johannesburg, South Africa

<sup>4</sup> Faculty of Health Sciences, University of the Witwatersrand, Johannesburg

**Corresponding author:** J Klaaren ([jonathan.klaaren@wits.ac.za](mailto:jonathan.klaaren@wits.ac.za))

In response to the COVID-19 pandemic, South Africa (SA) has established a Tracing Database, collecting both aggregated and individualised mobility and locational data on COVID-19 cases and their contacts. There are compelling public health reasons for this development, since the database has the potential to assist with policy formulation and with contact tracing. While potentially demonstrating the rapid facilitation through technology of an important public service, the Tracing Database does, however, infringe immediately upon constitutional rights to privacy and heightens the implications of ethical choices facing medical professionals. The medical community should be aware of this surveillance innovation and the risks and rewards it raises. To deal with some of these risks, including the potential for temporary rights-infringing measures to become permanent, there are significant safeguards designed into the Tracing Database, including a strict duration requirement and reporting to a designated judge. African states including SA should monitor this form of contact tracing closely, and also encourage knowledge-sharing among cross-sectoral interventions such as the Tracing Database in responding to the COVID-19 pandemic.

*S Afr Med J.* Published online 4 June 2020. <https://doi.org/10.7196/SAMJ.2020.v110i7.14852a>

## Responding to a pandemic

While the size and form of the COVID-19 pandemic in African states cannot be accurately predicted, it is clear that its effects will be significant. At the time of writing, most African governments were urgently responding in order to contain and mitigate the pandemic. In South Africa (SA), the crisis has sparked a number of initiatives, including several intersectoral co-ordination efforts such as a block exemption from the Competition Act No. 89 of 1998 for firms in the healthcare sector, in order to respond quickly and at scale to the novel coronavirus.<sup>[1]</sup>

One SA initiative was the establishment and regulation of a COVID-19 Tracing Database on 2 April 2020, building on the earlier development in March that linked a range of data warehouses as a research tool at the Council for Scientific and Industry Research (CSIR), a public body.<sup>[2,3]</sup> The purpose of the Tracing Database is 'to enable the tracing of persons who are known or reasonably suspected to have come into contact with any person known or reasonably suspected to have contracted COVID-19'.

Case and case-contact tracing and isolation are important in responding to the pandemic. They also comprise one of the essential elements of an exit strategy for a phased lifting of lockdown regulations, which have serious structural and long-term consequences for the economy and society. As well as these rewards, there are risks and potential dangers with the establishment of the database. Contact tracing through the collection of mobile data in order to identify and locate individuals necessarily involves a serious invasion of the constitutional right to privacy.

The establishment of the database also heightens the implications of the ethical choices made by professionals and others in the medical community attempting to ensure a balance between dealing

with a public health crisis on the one hand and protecting privacy on the other. While we do not directly address the ethical tensions presented by the pandemic in clinical settings, others have recently done so.<sup>[4]</sup> Doctors as custodians of patient-provider confidentiality should be thinking about the issues of public policy raised by the establishment of the Tracing Database and how it may play out going forward. Indeed, they need to disclose to the patients they are testing or sending for testing for SARS-CoV-2 that the patients' information will be disclosed to the database and kept confidential.<sup>[5]</sup> While current National Institute for Communicable Diseases contact tracing guidance incorporates ethical codes and confidentiality, it does not specifically take into account or reflect the establishment of the Tracing Database.<sup>[6]</sup> One specific recommendation flowing from our analysis is that this guidance should be revised in light of the database's establishment.

Beyond the immediate rewards and risks and the ethical issues presented, the establishment of the Tracing Database has potentially long-term consequences in fields such as law enforcement and financial services, as well as public health. It is therefore important to understand the establishment of the Tracing Database and to identify the specific limits and controls contained in the empowering regulations for it. After doing so, we further discuss the risks and rewards of the database, with specific attention to issues of privacy and ethics, and conclude by suggesting that its mode of implementation will be crucial to its success.

## The COVID-19 Tracing Database

The Tracing Database includes information on names, identity or passport numbers, cellphone numbers and test results of persons tested for COVID-19 and their known or suspected contacts. Data

are generated for this system from private and public laboratories and testing facilities, places of accommodation, and, perhaps most significantly, electronic communications service providers. For the first time, SA mobile phone companies have been placed under a generally applicable legal obligation to provide customer information to a state surveillance scheme. Mobile phone operators are required to promptly provide 'the location or movements of any person known or reasonably suspected to have contracted COVID-19; and the location or movements of any person known or reasonably suspected to have come into contact, during the period 5 March 2020 to the date on which the National State of Disaster has lapsed or has been terminated, with [such persons]'.<sup>[2]</sup> The data provided are likely to reproduce any errors currently captured by the operators under the terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. Similarly, the geographical data available from cellular service tower records will cover large areas. In both cases, it is important that the data subject have access to processes that can review and correct errors.

The legal regulations establishing the Tracing Database (see below) clearly envision and authorise the use of individualised data for contact tracing. Significantly and interestingly, this use goes beyond the initial reported intention of the CSIR – to aggregate location data for analytical purposes to provide evidence for rational crisis response and policy-making.

Below we discuss possible rights violations and ethical implications associated with the use of this location and movement information for case and case contact tracing.

The institutional and legal precedent for this reporting is the Notifiable Diseases Surveillance System. Notification has been relied upon as a method to track and control communicable diseases and manage outbreaks, and has had success.<sup>[7]</sup> Nonetheless, a series of recent studies has raised questions about the efficacy of this system in SA and internationally, noting poor perceptions of the system by stakeholders, lack of compliance by healthcare providers, and other concerns.<sup>[8-10]</sup>

## Privacy protections

A significant design feature of the Tracing Database is its built-in privacy protections. The information in the database is confidential and may only be used for the contact tracing purpose, and there are penalties for disclosure. The database is to incorporate all contact tracing information obtained from the mobile phone operators. If information obtained is not relevant to the database purpose, the National Department of Health (NDoH) may not retain that information beyond a period of 6 weeks. Furthermore, the information contained in the database must be de-identified within 6 weeks of the termination of the national State of Disaster and retained thereafter only for research, teaching and study purposes.<sup>[2]</sup>

Perhaps the most significant and certainly the most prominent privacy protection is the establishment of a COVID-19 Designated Judge to receive weekly reports on the location and movements information received from the mobile phone operators, as well as to recommend and report upon the winding down of the Tracing Database. Moreover, in what may well lead to notification to individual persons of their having being surveilled, the Judge is authorised 'to give directions as to any further steps to be taken to protect the right to privacy of those persons whose data has been collected, which directions must be complied with'. This last-mentioned power apart, the Designated Judge is perhaps more akin to a judge heading a judicial commission of inquiry than those judges adjudicating on warrant requests in terms of SA's

operative surveillance law.<sup>[11]</sup> Other than receiving weekly reports and making directions upon receiving the final winding-up report, the chief power and function of the Designated Judge is to suggest improvements to the Tracing Database directly to Cabinet through a recommendation and regulation amendment process provided for in Regulation 11H(15).<sup>[2]</sup>

In the SA legal context, the Tracing Database takes place under a legislatively authorised National State of Disaster (not a State of Emergency) in a constitutional democracy. As detailed above, its institutional protections for privacy are significant. Nonetheless, the Tracing Database poses risks both to the rule of law and to the protection of individual rights at the same time as it offers opportunities for an effective pandemic response. The relevant Minister's declaration of a National State of Disaster authorises her to issue regulations together with other ministers in various sectors and provides for 'directives' by such ministers.<sup>[12]</sup> One safeguard is that these regulations and directives and actions taken in their terms will need to be justifiable under the Bill of Rights and survive judicial scrutiny under the principle of legality (or the administrative justice statute if the regulations are deemed to constitute administrative action). However, there may be a strong case for *ex post* legislative controls in the form of a parliamentary reporting requirement, in part to facilitate public deliberation and education on such issues of great import and long-term significance.

SA has experience establishing and applying the standards of lawfulness to wide, broad, and potentially vague grants of discretionary power under the two States of Emergency in the 1980s (which demonstrated the real dangers of the persistence of 'temporary' rights-infringing measures).<sup>[13]</sup> Progressive lawyers made very creative challenges to the emergency regulations without the aid of a Bill of Rights, such as the SA Constitution now includes.<sup>[14]</sup> Medical professionals also at times directly responded to the States of Emergency and their effects on health.<sup>[15-17]</sup> The current political and legal context is substantially different – a constitutional democracy responding to a public health crisis, not an instance of state repression. The COVID-19 National State of Disaster is the first time in our post-apartheid history that there have been such broad grants of discretionary powers to government officials. Yet the state must comply with constitutional standards of legality and rights. So far, indications are that courts will exercise extreme caution before intervening, at least for as long as the state can give assurances that it is acting on the basis of scientific evidence and the advice of healthcare professionals. We have, however, already seen instances of the abuse of policing powers. So the question of the approach the courts will adopt to enforcement of the rule of law and rights protection under a 'State of Disaster' is critically important.

## Regulating the risks and rewards of the tracing database

The Tracing Database initiative occupies an emerging global regulatory space, at the intersection of public health, constitutional rights during emergencies and disasters, credit surveillance, open data, and information privacy.<sup>[18-22]</sup> Widespread laws, including the National Credit Act 34 of 2005 in SA, have provided a legal basis for individualised surveillance in the field of credit and finance. The emerging global regulatory guidance for the COVID-19 pandemic is fairly clear that aggregated data, with appropriate restrictions, can and should be used as far as effective in order to combat the pandemic and calibrate mitigation and anti-transmission measures.<sup>[19,23]</sup> While still emerging, this regulatory guidance emphasises that uses of individualised data infringe upon rights and therefore, for instance,

recommends that any use of contact tracing applications be voluntary.<sup>[24]</sup> The SA regulator charged with data protection has issued a Guidance Note addressing the Tracing Database which stipulates that the mobile phone operators should provide location-based data of data subjects if such provision complies with an obligation imposed by law (such as the regulations described above).<sup>[25]</sup> However, 'the Government must still comply with all the applicable conditions for the lawful processing as set out in this Guidance Note.'<sup>[25]</sup>

The use of individualised data, as in the Tracing Database, poses higher privacy and ethical concerns than the use of aggregated data. It may also have different, more targeted, and in certain situations more effective impacts. It is therefore worthwhile to identify specific uses to which the Tracing Database could be put that would raise very high concerns of privacy and other rights concerns. One such example might be in relation to mandated quarantines.<sup>[26,27]</sup> Data in the Tracing Database might be shared with law enforcement to monitor and enforce compliance by individuals with mandated quarantines. Most legal commentators feel that health officials 'would be justified in the public interest, in arresting and detaining, quarantining or isolating, any person who is suspected or is carrying a communicable disease.'<sup>[28]</sup> One SA court has grappled with quarantine in the context of drug-resistant tuberculosis.<sup>[29]</sup> A rights-respecting Tracing Database will require sensitive, informed and non-violent implementation of restrictions of persons' movements if they are found to be possibly infected or able to infect others. Medical professionals will inevitably be faced with choices for which there is no specific regulatory or ethical guidance. The mode of rights-regarding and ethically aware implementation we are calling for has been demonstrably lacking in numerous reported actions of the South African National Defence Force (SANDF) and the police to date. The deployment of additional SANDF troops to police the lockdown and reports of cases of abuse of power underline how important it is to protect individuals' rights.<sup>[30-32]</sup>

## After establishment

Actions taken to implement the Tracing Database will be crucial to its success and its social reception. Indeed, technological and regulatory choices will be at the same time critical and inevitably political. Whether those charged with building and using the CSIR databases focus on the use of call detail records (which provide the billing details of voice calls) or usage detail records (which specify the connections between phone devices and the cellular providers' towers without requiring voice calls), the surveillance will be able to create origin-destination matrices, dwell estimations and hotspots, time at work/home estimates, and contact matrices. These should equip the NDoH and the SA government with a central point to read the progress of the pandemic and its recession on a national scale.<sup>[19]</sup> Real-time phone metadata – which had been available to the police with a judicial warrant under existing surveillance laws<sup>[33]</sup> – are being combined with the existing notifiable disease regime. The obligation imposed on the telecommunications firms by the regulation may produce a real-time government surveillance database for the first time. The development of and adherence to standards of privacy protection and ethics in implementing a large limited-duration government-led project such as this one requires appropriate investment, systems, and confidentiality agreements as well as good technical warehouse capacity. The experience of the Competition Commission's Health Market Inquiry in obtaining, deidentifying, analysing and safeguarding personal information in the healthcare sector may well be helpful here.<sup>[34]</sup>

Over and above attention to the critical choices to be made in the implementation of the Tracing Database, we argue that oversight

on rights infringements is as important. Current safeguards do not actively involve civil society, including structures of the medical professions. Many civil society organisations are currently active during the State of Disaster,<sup>[35]</sup> and could be central to the database implementation process in order both to safeguard rights and to ensure the efficacy of contact tracing through bolstered public trust and legitimacy. The CSIR and the NDoH should work actively to involve civil society in the implementation of the database as well as in the foreseen activities of research after the State of Disaster. Fundamentally we argue that while the public may tolerate this degree of invasion of privacy under particular circumstances, there is a danger that it will become normalised, and the exceptional nature of infringements of individual rights needs to be underscored. Public debate, participation, and education on these privacy and ethical issues is important in a rights-based constitutional democracy. In our view, healthcare providers and their organisations have a particular responsibility to ensure that rights violations are avoided during this pandemic. Other states in the rest of Africa and in the rest of the world may be able to learn and adapt from the SA response,<sup>[32]</sup> as well as to contribute their own experience and knowledge to improve the SA response and to develop a repertoire of context-specific and effective responses to the pandemic.

**Declaration.** None.

**Acknowledgements.** The helpful comments of the *SAMJ* reviewer are appreciated.

**Author contributions.** This article was initiated by JK. KB, FC, SF and MV contributed conceptually to the article and reviewed all versions submitted to the journal.

**Funding.** National Research Foundation, Mellon Foundation.

**Conflicts of interest.** None.

1. Nkonki L, Fonn S. Decisive and strong leadership and intersectoral action from South Africa in response to the COVID-19 virus. *S Afr Med J* 2020;110(5):339-340. <https://doi.org/10.7196/SAMJ.2020.v110i5.14739>
2. Department of Co-operative Governance and Traditional Affairs. Disaster Management Act, 2002: Amendment of regulations issued in terms of section 27(2). Government Gazette No. 43199, 2 April 2020. (Published under Government Notice No. R. 446). [https://www.gov.za/sites/default/files/gcis\\_document/202004/43199rg11078-gon446.pdf](https://www.gov.za/sites/default/files/gcis_document/202004/43199rg11078-gon446.pdf) (accessed 29 May 2020).
3. SAnews (South African Government News Agency). Government sets up COVID-19 research data platform. 28 March 2020. <https://www.sanews.gov.za/south-africa/government-sets-covid-19-research-data-platform> (accessed 6 April 2020).
4. Behrens KG. Clinical ethical challenges in the Covid-19 crisis in South Africa. *Wits J Clin Med* 2020;2(SI):29-32. <https://doi.org/10.18772/26180197.2020.v2nSIa5>
5. McQuoid-Mason DJ. COVID-19 and patient-doctor confidentiality. *S Afr Med J* 2020;110(6):461-462. <https://doi.org/10.7196/SAMJ.2020.v110i6.14797>
6. National Institute for Communicable Diseases, Department of Health (South Africa). Coronavirus disease 2019 (COVID-19) caused by a novel coronavirus (SARS-CoV-2): Guidelines for case-finding, diagnosis, management and public health response in South Africa. Version 2.0. Updated 8 March 2020. [https://www.nicd.ac.za/wp-content/uploads/2020/03/NICD\\_DoH\\_COVID-19\\_Guidelines\\_8\\_March\\_2020\\_final.pdf](https://www.nicd.ac.za/wp-content/uploads/2020/03/NICD_DoH_COVID-19_Guidelines_8_March_2020_final.pdf) (accessed 29 May 2020).
7. Clarkson JA, Fine PEM. The efficiency of measles and pertussis notification in England and Wales. *Int J Epidemiol* 1985;14(1):153-168. <https://doi.org/10.1093/ije/14.1.153>
8. Benson F, Musekiwa A, Blumberg L, Rispel L. Comparing laboratory surveillance with the notifiable diseases surveillance system in South Africa. *Int J Infect Dis* 2017;59:141-147. <https://doi.org/10.1016/j.ijid.2017.03.007>
9. Benson FG, Levin J, Rispel LC. Health care providers' compliance with the notifiable diseases surveillance system in South Africa. *PLoS ONE* 2018;13(4):e0195194. <https://doi.org/10.1371/journal.pone.0195194>
10. Benson FG, Musekiwa A, Blumberg L, Rispel LC. Survey of the perceptions of key stakeholders on the attributes of the South African Notifiable Diseases Surveillance System. *BMC Public Health* 2016;16(1):1120. <https://doi.org/10.1186/s12889-016-3781-7>
11. South Africa. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. Southern African Legal Information Institute, last checked 30 October 2019. [http://www.saflii.org/za/legis/consol\\_act/roicopocia2002943/](http://www.saflii.org/za/legis/consol_act/roicopocia2002943/) (accessed 15 April 2020).
12. South Africa. Disaster Management Act 57 of 2002. <http://www.lawsofsouthafrica.up.ac.za/index.php/current-legislation> (accessed 29 May 2020).
13. Mathews AS, Albino RC. The permanence of the temporary – and examination of the 90- and 180-day detention laws. *S Afr Law J* 1966;83(1):16-43. <https://heinonline.org/HOL/PP?h=hein.journals/soaf83&i=34> (accessed 15 April 2020).
14. Ellmann S. In a Time of Trouble: Law and Liberty in South Africa's State of Emergency. Oxford: Clarendon Press, 1992.
15. Baldwin-Ragaven L, London L, Gruchy JD. An Ambulance of the Wrong Colour: Health Professionals, Human Rights and Ethics in South Africa. Cape Town: Juta & Co., 1999.

16. Orr W. Health and human rights: A South African experience. *Can Fam Physician* 2002;48(12):1880-1883. <https://www.cfp.ca/content/48/12/1880> (accessed 29 May 2020).
17. McLean GR, Jenkins T. The Steve Biko affair: A case study in medical ethics. *Dev World Bioeth* 2003;3(1):77-95. <https://doi.org/10.1111/1471-8847.00060>
18. Buckee CO, Balsari S, Chan J, et al. Aggregated mobility data could help fight COVID-19. *Science* 2020;368(6487):145-146. <https://doi.org/10.1126/science.abb8021>
19. Oliver N, Letouzé E, Sterly H, et al. Mobile phone data and COVID-19: Missing an opportunity? *arXiv:2003.12347* [cs.CY]. 27 March 2020. <https://arxiv.org/abs/2003.12347> (accessed 29 May 2020).
20. Raskar R, Schunemann I, Barbar R, et al. Apps gone rogue: Maintaining personal privacy in an epidemic. *arXiv:2003.08567* [cs.CR]. 19 March 2020. <http://arxiv.org/abs/2003.08567> (accessed 24 March 2020).
21. Global Research Collaboration for Infectious Diseases Preparation. Principles of data sharing in public health emergencies. June 2018. <https://www.glopid-r.org/wp-content/uploads/2018/06/glopid-r-principles-of-data-sharing-in-public-health-emergencies.pdf> (accessed 24 March 2020).
22. Staunton C, Adams R, Anderson D, et al. Protection of Personal Information Act 2013 and data protection for health research in South Africa. *Int Data Priv Law* 2020;ipz2024. <https://doi.org/10.1093/idpl/ipz2024>
23. European Data Protection Board. Statement on the processing of personal data in the context of the COVID-19 outbreak. 19 March 2020. [https://edpb.europa.eu/sites/edpb/files/files/news/edpb\\_statement\\_2020\\_processingpersonaldataandcovid-19\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf) (accessed 24 March 2020).
24. 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. [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_20200420\\_contact\\_tracing\\_covid\\_with\\_annex\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf) (accessed 14 May 2020).
25. Information Regulator (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). 2020. <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPi-Covid19-20200403.pdf> (accessed 29 May 2020).
26. Botes WM, Thaldar DW. COVID-19 and quarantine orders: A practical approach. *S Afr Med J* 2020;110(6):469-472. <https://doi.org/10.7196/SAMJ.2020.v110i6.14794>
27. Moodley K, Obasa AE, London L. Isolation and quarantine in South Africa during COVID-19: Draconian measures or proportional response? *S Afr Med J* 2020;110(6):456-457. <https://doi.org/10.7196/SAMJ.2020.v110i6.14842>
28. Kirby N. Patient mobility migration and mitigation – the devil and the deep blue sea. *Med Law* 2009;28(4):673-688. <https://heinonline.org/HOL/P?h=heinjournals/mlv28&i=703> (accessed 15 April 2020).
29. Pieterse M, Hassim A. Placing human rights at the centre of public health: A critique of Minister of Health, Western Cape v. Goliath. *S Afr Law J* 2009;126(2):231-245. <https://heinonline.org/HOL/P?h=heinjournals/soaf126&i=237> (accessed 29 May 2020).
30. The Defense Post. South Africa to deploy 73,000 more troops to enforce COVID-19 lockdown. 22 April 2020. <https://www.thedefensepost.com/2020/04/22/south-africa-deploy-73000-troops-covid-19-lockdown/> (accessed 24 April 2020).
31. South African Government. Parliament receives report from police and IPID on coronavirus COVID-19 lockdown. 17 April 2020. <https://www.gov.za/speeches/parliament-receives-report-police-and-ipid-coronavirus-covid-19-lockdown-%C2%A0-17-apr-2020-0000> (accessed 24 April 2020).
32. Nicholl DJ, Jenkins T, Miles SH, Hopkins W, Siddiqui A, Boulton F. Biko to Guantanamo: 30 years of medical involvement in torture. *Lancet* 2007;370(9590):823. [https://doi.org/10.1016/S0140-6736\(07\)61402-0](https://doi.org/10.1016/S0140-6736(07)61402-0)
33. Hunter M. Cops and call records: Policing and metadata privacy in South Africa. Media Policy and Democracy Project, March 2020. [https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/cops\\_and\\_call\\_records\\_web\\_masterset\\_26\\_march.pdf](https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/cops_and_call_records_web_masterset_26_march.pdf) (accessed 31 March 2020).
34. Health Market Inquiry. Final Findings and Recommendations Report. September 2019. <http://www.compcom.co.za/wp-content/uploads/2020/01/Final-Findings-and-recommendations-report-Health-Market-Inquiry.pdf> (accessed 7 April 2020).
35. Peacock T, Hodgson TF, Quinn C, van Leeve Y, Kathi T. The law during a state of disaster and human rights risks. C19 People's Coalition, 2020. <https://c19peoplescoalition.org.za/wp-content/uploads/2020/04/the-law-during-a-state-of-disaster-and-human-rights-risks.pdf> (accessed 29 May 2020).

*Accepted 27 May 2020.*