

Track and trace, trial and error

Assessing South Africa's approaches to
privacy in Covid-19 digital contact tracing



The Media Policy and Democracy Project

Murray Hunter

Track and trace, trial and error

Assessing South Africa's approaches to privacy in Covid-19 digital contact tracing

The Media Policy and Democracy Project

Digital contact tracing has been at the centre of global concerns about privacy and digital rights during the Covid-19 pandemic. In March 2020, South Africa joined dozens of other countries in looking for sophisticated technological solutions to aid its contact-tracing efforts, with an ambitious if misguided attempt to use locational data from mobile-network operators to help 'track and trace' people with the virus.

While the programme was misconceived – officials abandoned the attempt to use cellular data for contact tracing after just a few weeks – it did yield a novel set of privacy protections designed to ensure oversight and safeguard against its misuse. In doing so, South Africa appeared in one way to eschew a common global narrative about privacy in the pandemic: that crises provoke emergency powers that are only ever excessive, expansive and ever-lasting.

Since then, South Africa's health authorities' evolving approach to contact tracing has shifted to a range of other digital interventions that seem more carefully considered, but that have often been put into effect with little public consultation and haphazard transparency.

This report attempts to piece together a public record (albeit incomplete) of how the initial digital contact-tracing policy was created, why it failed, and what came next. In doing so it gives a first assessment of some the privacy and data protection issues that emerged, and a critical reflection on the challenges of policy making in a time of crisis, where well-intentioned officials grapple with complex problems under immense pressure.

It draws on interviews and correspondence with a range of officials from public bodies and industry, in many instances on the condition of anonymity because they did not have authorisation to speak publicly. This includes initial fact-gathering undertaken in March 2020 in my capacity then as acting advocacy coordinator of the amaBhungane Centre for Investigative Journalism.

Murray Hunter | murray@c1rcloup.org

November 2020

My thanks goes to all who participated in this research, including those who may disagree with its findings.

I would also like to acknowledge valuable help from David Johnson, Marielle Wenger, Elri Voigt, Avani Singh, Michael Power, Alexandrine Pirlot de Corbion, Eva Blum-Dumontet, Jane Duncan, Chereese Thakur and the amaB team, and two long-suffering humans at home

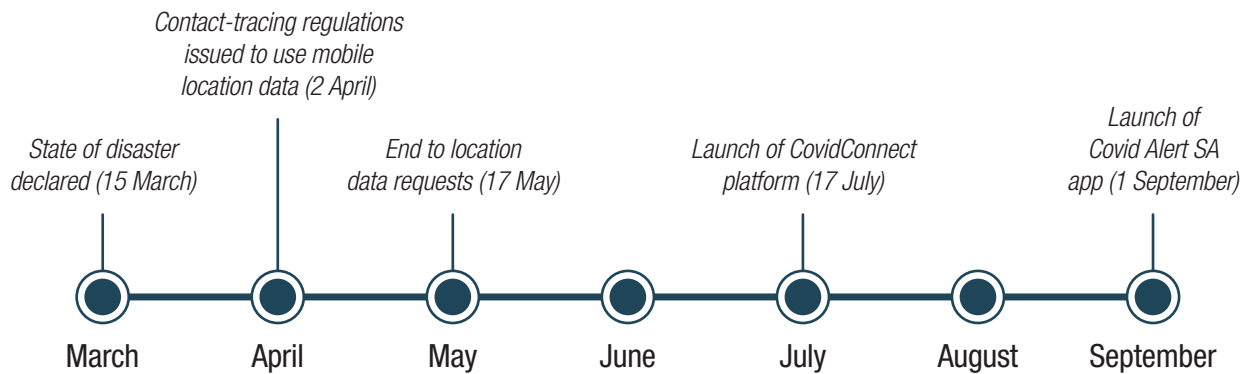
Cover image by Elmond Jiyane, Government Communication and Information System

Contents

Introduction	1
The opportunities and risks of digital approaches	4
Scepticism about surveillance powers in South Africa	6
The directive from Communications	8
Health authorities' early thinking on contact tracing	11
Unpacking the April regulations	12
Abandoning the 'location-tracking' approach	17
What went wrong?	20
Misunderstanding of the technology	20
Misreading international responses.....	20
Limited external feedback	21
Missing fundamentals?.....	22
What went right?	23
The shift to other approaches	26
CovidConnect	26
The Bluetooth app	27
Aggregate mobile data	28
Further problems with the regulations	30
Keeping mobile network contact tracing 'on the books'	30
Expanding the purpose for data collection.....	31
The lessons for privacy	33
Recommendations	36
References	38

1

Introduction



Contact tracing is an essential public-health response whereby those who have been exposed to the novel coronavirus are identified and notified as quickly as possible so that they can isolate themselves¹ – became the subject of various digital technologies, prompting notorious debates about data protection and other surveillance risks versus the potential for these solutions to save lives.

In March 2020, in the weeks after its first confirmed cases of Covid19, South Africa joined dozens of other countries in looking for sophisticated technological solutions to aid its contact-tracing efforts. While different governments had experimented with a range of approaches,² the initial South African programme sought to use locational information from mobile-network operators to help ‘track and trace’ people with Covid-19 and those who had been exposed to them. Locational privacy is a vital principle in digital and communications privacy, because location data can be used to create very detailed and invasive records of a person’s movements, public and private activities, and personal contacts.³

¹ World Health Organisation, ‘Contact tracing in the context of COVID-19: interim guidance’, 10 May 2020, <https://www.who.int/publications/item/contact-tracing-in-the-context-of-covid-19>

² These include use of mobile network data or data from financial transactions to track down patients for quarantine, as well as apps to monitor people’s movements via GPS, or detect people’s proximity to one another via Bluetooth. See <https://privacyinternational.org/examples/location-data-and-covid-19>

³ A Blumberg & P Eckersley, ‘On locational privacy, and how to avoid losing it forever’, White Paper, Electronic Frontier Foundation, 2009, <https://www.eff.org/files/eff-locational-privacy.pdf>

South Africa's Constitution recognises the right to privacy in its Bill of Rights, including the right of everyone not to have the privacy of their communications infringed.⁴ It had also produced a data protection law, the Protection of Personal Information Act, which will come fully into force in July 2021 after considerable delays. In acknowledging the privacy risks of the proposed contact-tracing programme for Covid-19, in April 2020 the authorities unveiled a novel set of privacy protections designed to ensure oversight and safeguard against its misuse (the 'April regulations'). These April regulations included the appointment of a highly respected judge to oversee and review the workings of the system, as well as various transparency measures that in some respects were an improvement to South Africa's longstanding communications surveillance law, known as RICA. Indeed, the April regulations seemed to establish safeguards for South Africa's digital contact-tracing programme that appear to have been shaped by years of criticism, activism and public advocacy directed at state surveillance in democratic South Africa.

It has largely gone without public comment that the attempt to use location data from mobile networks failed almost from the start, with health authorities pivoting away from the approach barely six weeks after it was announced. Since then, South Africa's evolving approach to contact tracing has shifted to a range of other digital interventions – including through the messaging platform known as CovidConnect, and the Covid Alert Bluetooth-based app. These interventions seem more carefully considered, although I argue that they have often been implemented with a lack of public consultation and with haphazard transparency.

As much as it was a policy failure in terms of its ineffectiveness, elements of the first policy represented a step forward for how the South African state thinks about privacy safeguards. At the same time, at its heart the digital contact-tracing initiative was arguably borne from technological 'solutionism' – a policymaking tendency that seeks out improbable technological 'fixes' to complex problems. This, I would argue, has been a common feature of governments' responses to the pandemic, and many other governance challenges as well.

⁴ Constitution of Republic of South Africa, 1996, sec 14.

This paper attempts to piece together a basic public record of how the policy was created, why it failed, and what came next. It draws on interviews and correspondence with a range of officials from public bodies and industry, in many instances on the condition of anonymity because they did not have authorisation to speak publicly. This is necessary in the first instance because there has been a lack of public disclosure and investigative research on this small part of the broader South African response to Covid-19. Then the paper will attempt a critical assessment of the events surrounding South Africa's first attempts at digital contact tracing, and what lessons can be drawn for privacy protections and policy making in a time of crisis.

In doing so, this research aims to contribute to a critical assessment of the lessons can be drawn for privacy protections and policy making in a time of crisis, where well-intentioned officials grapple with complex problems under immense pressure.

2

The opportunities and risks of digital approaches

In South Africa, ‘manual’ contact tracing was coordinated at a provincial level and district level, so approaches varied, but generally appears to have been undertaken through a combination of volunteers and healthcare workers in ‘call centre’ setups.

The case for digital contact tracing stems from the virus’s notorious infectiousness. Contact tracing is recognised as one crucial strategy to contain the spread of infections, but it is a labour-intensive process.⁵ An influential modelling exercise published in *Science* found that the process needs to be fast and fairly comprehensive to work. If most contacts of known Covid-19 cases could be notified and isolated in less than a day, the spread of infections slows dramatically; if the process drags out to just three days, it does little to contain the epidemic.⁶ The researchers behind this model concluded that this result is unlikely to be achieved at scale without reliance on digital and automated contact tracing, such as through an app.

In a June 2020 guidance note, the World Health Organisation recognised the potential for digital tools to augment or automate contact tracing efforts, with the caveat that there was still limited evidence to measure the effectiveness of such interventions – and that in any case these could only be effective as part of a much broader public-health infrastructure which includes well-staffed health services, rapid testing, and manual contact tracing capacity.

As ever, the potential for tech-driven health initiatives comes with caveats: interventions that rely on people’s access to digital technology may amplify socioeconomic and healthcare inequalities, and often bear huge risks to privacy and other human rights.⁷

There was early awareness of the risk that emergency responses to the pandemic by governments could wittingly or unwittingly result in lasting damage to human rights and the democratic climate of their societies. In March 2020, a panel of UN Special Rapporteurs

5 For example, an account from the early days of South Africa’s pandemic followed the efforts of a team of 20 contact tracers working into the night to track down more than 1000 people exposed to the virus at a mass church gathering. See Bhekisisa Centre for Health Journalism, ‘Can you pause a pandemic? Inside the race to stop the spread of COVID-19 in South Africa’, 26 March 2020, <https://bhekisisa.org/features/2020-03-26-can-you-pause-a-pandemic-inside-the-race-to-stop-the-spread-of-covid19-in-south-africa/>

6 L. Ferretti and others, ‘Quantifying SARS-CoV2 transmission suggests epidemic control with digital contact tracing’, *Science*, 368, 6491, 8 May 2020, DOI: 10.1126/science.abb6936

7 U Gasser and others, ‘Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid’, *Lancet Digital Health*, 2020, 2, 29 June 2020, [https://doi.org/10.1016/S2589-7500\(20\)30137-0](https://doi.org/10.1016/S2589-7500(20)30137-0)

and independent experts issued a statement calling for world governments to ensure their pandemic responses upheld basic human rights, and warned against the use of emergency measures to quash dissent or to take legal or political shortcuts which could allow ‘excessive powers to become hardwired into legal and political systems.’⁸ While a focus on state excesses is understandable given the fundamental role of national governments in leading public-health responses, the pandemic era has also come with new opportunities for global tech giants and smaller industry players alike to angle for influence and profit.⁹

With the first confirmed Covid-19 case on 5 March 2020, the arrival of the pandemic in South Africa sparked a rapid and intensive response from government. Within 10 days of the first confirmed case, the President declared a national state of disaster. Under the Disaster Management Act, the President announced that the country would go into a hard lockdown on 27 March, which would go on to last several months; cabinet ministers issued a cascade of new regulations and emergency policies, applying not only to conventional public-health matters but to many details of public life, from prescribed hours for exercise to the sale of hot food. Some parts of the state response were less trivial; the deployment of police and soldiers to the streets to enforce the lockdown resulted in widespread reports of brutality and harassment, and at least ten deaths.¹⁰ Thus, while aspects of South Africa’s response to the pandemic earned the praise of the World Health Organisation and others,¹¹ at least some parts of government’s response seemed to confirm fears that the crisis would result in securocratic excesses.¹²

Against this backdrop sits South Africa’s approach to contact tracing, where initial analyses tended to frame the initial intervention as falling within a global trend either of high-tech health innovation or worrying surveillance overreach.

8 UN Office of the High Commissioner on Human Rights, COVID-19: States should not abuse emergency measures to suppress human rights – UN experts, 16 March 2020, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E>

9 D Lyon, ‘The coronavirus pandemic highlights the need for a surveillance debate beyond “privacy”’, *The Conversation*, May 2020, <https://theconversation.com/the-coronavirus-pandemic-highlights-the-need-for-a-surveillance-debate-beyond-privacy-137060>

10 Viewfinder, ‘Details of two additional alleged lockdown killings by police revealed’, 30 April 2020, <http://viewfinder.org.za/details-of-two-additional-alleged-lockdown-killings-by-police-revealed/>

11 IOL, ‘Coronavirus in SA: WHO boss praises South Africa’s response to Covid-19 pandemic’, 1 April 2020, <https://www.iol.co.za/news/politics/coronavirus-in-sa-who-boss-praises-south-africas-response-to-covid-19-pandemic-45923836>

12 See New Frame editorial, ‘South Africa faces a stark political choice’, 29 May 2020, <https://www.newframe.com/south-africa-faces-a-stark-political-choice/>

3

Scepticism about surveillance powers in South Africa

The concern that South African authorities would abuse a new spying power was far from theoretical. When he assumed office in 2018, President Cyril Ramaphosa launched a review of the State Security Agency, which found damning evidence of criminality and abuse of power within the intelligence structures.¹³ This followed a pattern of documented abuses of the state's existing communications surveillance powers, in which security agencies – and individual officials within them – took advantage of weak safeguards, lack of oversight and legal loopholes to spy on various adversaries, including journalists, anti-corruption investigators, and perceived political rivals.¹⁴

Pertinent to digital tracking during Covid-19, this pattern of abuse included apparent abuses of access to locational privacy: while South Africa's main surveillance law, known as RICA,¹⁵ generally requires a judge to pre-authorise any interception of a person's communications or metadata, it also includes an emergency procedure to trace a person's number without the prior authorisation of a judge. Available data shows that police officials use this emergency procedure thousands of times every year without explanation.¹⁶ In some contexts, locational privacy is also a matter of personal safety. This point seems to have been chillingly made in the recent assassination of a senior police detective in Cape Town; state prosecutors allege that his assassins had tracked his movements through illicit access to his cellular location data.¹⁷

In February 2020, just weeks before South Africa recorded its first Covid-19 case, the Constitutional Court heard arguments in *amaBhungane*, a challenge to the constitutionality of the country's primary surveillance law, RICA, which resulted from a government spying operation against journalist Sam Sole.¹⁸

¹³ Presidency of the Republic of South Africa, 'High-level Review Panel Report on the State Security Agency', December 2018, <http://www.thepresidency.gov.za/download/file/fid/1518>

¹⁴ M Hunter, 'Cops and call records: Policing and metadata privacy in South Africa', Media Policy and Democracy Project, 2020, <https://mediaanddemocracy.com/>

¹⁵ The full title of RICA is the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

¹⁶ J Duncan, *Stopping the spies: Constructing and resisting the surveillance state in South Africa*. Johannesburg: Wits University Press, 2018, 101.

¹⁷ Daily Maverick, 'Common cellphone tracking service used in ambush and murder of top policeman Kinnear', 23 September 2020, <https://www.dailymaverick.co.za/article/2020-09-23-common-cellphone-tracking-service-used-in-ambush-and-murder-of-top-policeman-kinnear/>

¹⁸ *amaBhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others*, CCT 278/19.

At the time of writing, judgment in the Constitutional Court is still pending, but the High Court had previously ruled overwhelmingly in amaBhungane's favour, ordering major changes to the Act which would boost transparency and oversight on how the state undertakes communications surveillance. If upheld by the Constitutional Court, these provisional changes would be a significant move to address well-documented weaknesses in the privacy safeguards established in RICA.

Of particular note is that the court ordered that RICA should be amended to include a 'user notification' provision, meaning that people whose communications are intercepted under RICA should generally be notified after the fact.¹⁹ This would strike down a secrecy provision in RICA which expressly prohibits any of the parties involved in an interception from 'tipping off' a target of the interception, even after an investigation has been concluded. User notification is a basic feature of international standards for such laws;²⁰ critics of RICA had long argued that the lack of post-surveillance notification in South Africa's surveillance law had helped spying abuses to go undetected.²¹

¹⁹ amaBhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others (25978/2017) [2019] ZAGPPHC 384; [2019] All SA 343 (GP); 2020 (1) SA 90 (GP), 16 September 2019.

²⁰ See African Commission on Human and Peoples' Rights, Declaration of principles of freedom of expression and access to information in Africa, 2019; The International Principles on the Application of Human Rights to Communications Surveillance, 2014, <https://necessaryandproportionate.org/>

²¹ M Hunter, 'Open letter to Bheki Cele, RICA victim', News24, 25 February 2020, <https://www.news24.com/news24/Columnists/GuestColumn/open-letter-to-bheki-cele-rica-victim-20200225>

4

The directive from Communications

8. INDIVIDUAL TRACK AND TRACE

- 8.1 The Electronic Communication Network Service (ENCS) and Electronic Communication Service (ECS) Licensees, internet and digital sector in general, must provide location-based services in collaboration with the relevant authorities identified to support designated departments to assist and combat the spread of COVID-19.

A week before the release of the ‘April regulations’ on contact tracing, another government department had provoked significant privacy concerns when it announced the first proposal to use cell phone data to track the spread of Covid-19 in South Africa. This came from the Minister of Communications and Digital Technologies, who issued a set of directions to the communications industry just a few hours before South Africa’s first hard lockdown was set to begin. It included a paragraph under the heading ‘Track and Trace’:

The Electronic Communication Network Service (ENCS) and Electronic Communication Service (ECS) licensees, internet and the digital sector in general are directed to provide location-based services in collaboration with the relevant authorities identified to support designated departments to assist and combat the spread of COVID-19.²²

The directive appeared to confirm fears that the public-health crisis would result in expansive surveillance powers²³, though in retrospect it appeared the officials involved had largely been oblivious to the privacy implications of their proposal. Yet in its vagueness, the drafting left much open to interpretation: was this a provision to track individuals’ locations via communications networks, or for the state to get aggregate network data to measure population movements?

²² Minister of Communications and Digital Technology, Directions, GN 417, 26 March 2020.

²³ A Singh & M Power, ‘New digital regulations mean the state can track you – no questions asked,’ Mail & Guardian, 31 March 2020, <https://mg.co.za/article/2020-03-31-new-digital-regulations-mean-the-state-can-track-you-no-questions-asked/>

In a prior briefing, the had said mobile-network operators would provide ‘data analytics’ to help track the spread of the virus, although it was not clear if this would involve individuals’ location-data or aggregated network data.²⁴

Pressed for comment, South Africa’s largest mobile operators suggested that the companies would not deviate from their current obligations under law. In response to a telephonic inquiry at the time, I received a terse statement from MTN that read:

*MTN will continue to follow the standard legislated protocols for location based services as with any other such request that is made under normal (non-COVID-19) circumstances.*²⁵

A Vodacom spokesperson also emphasised that the company would not provide customer information outside of existing legal mechanisms, but speculated (incorrectly) that the Minister’s proposal would apply to aggregated network data:

*Having said that, our understanding of the data information request outlined yesterday by Minister Stella Ndabeni-Abrahams is for high-level aggregated data on how people are moving to help curb the spread of Covid-19. This does not include personal information or information that identifies a specific individual.*²⁶

However, in a television interview later that week, the Minister seemed to make clear that the policy was intended to allow for individualised tracking, and that the collective health emergency outweighed any risks to privacy or other civil liberties:

*As part of the regulations, we’re engaging the responsible departments, which is Justice [and] State Security to say, how do you make sure that we can contribute in terms of tracing individuals, as you know that when you’re going for the test, you fill in the form and put on your details. And then to say, we can know if this person has tested positive in this area, therefore, that information may be provided so that we can trace it per area and say in this area, these are the individuals that are there. [...] But of course we’re in engagement with the Department of Justice on this to say how legal it will be in our case, but also, do appreciate the fact that we’re operating under the Disaster Management Act. We are working together to say, What are other methods can we introduce to make sure that you can help, because it is also **not***

²⁴ Oral briefing by Minister of Communications and Digital Technology, 24 March 2020.

²⁵ Email from Jacqui O’Sullivan, MTN spokesperson, on 26 March 2020.

²⁶ Email from Byron Kennedy, Vodacom spokesperson, on 26 March 2020.

good that we want to protect only the rights of individuals at the expense of the rights of the country. In this instance, we're looking at the only right that matters for now: the right to have life [emphasis added].²⁷

In this initial foray by the Minister of Communications, it appeared that South Africa was set to follow the worst impulses of crisis-driven policy making. With a single paragraph of its policy directive, her department had proposed to enact an unprecedented expansion of the state's power to access people's communications data – with no provisions for oversight, limits or safeguards, and little evidence that protections for the right to privacy had been considered at all. Even under RICA – an interceptions law which faces very real prospects of being struck down as unconstitutional – such information is treated as sensitive enough that the police and intelligence agencies would only be granted access under very limited circumstances, and generally only with the prior approval of a judge or magistrate.²⁸

Yet if this policy move would have the effect of expanding the state's surveillance capability, there was little evidence that it was the result of a cynical 'power grab' on the part of authorities. Rather, my engagements with officials around the Ministry and Department seemed to suggest that there had been limited consideration of the privacy implications for the proposed scheme, or how it would depart from existing laws.

For example, a spokesperson for the Minister seemed nonplussed by concerns that this policy had implications for privacy – on the basis that authorities would only be seeking users' locational data, as opposed to 'sensitive' information, and could say little about whether the drafters had considered existing legal safeguards for privacy.²⁹

In any case, within a week this policy directive by the Minister of Communications would be replaced. A much more detailed set of regulations issued on 2 April by the Ministry of Cooperative Governance and Traditional Affairs, had been driven by the Department of Justice and legal advisors within the Presidency – with no involvement, either in the drafting of the policy or in the policy itself, of the Ministry of Communications. Where the preceding directive had been a single paragraph, the new regulations ran to four pages, and contained significant detail on privacy protections and oversight.

²⁷ S Ndabeni-Abrahams, Interview on SABC Morning Live, 25 March 2020.

²⁸ M Hunter, 'Digital privacy in the time of pandemics,' amaBhungane, 31 March 2020, <https://amabhungane.org/advocacy/advocacy-comment-digital-privacy-in-the-time-of-pandemics/>

²⁹ Email from Nthabaleng Mokitimi, spokesperson for the Minister, on 27 March 2020.

Health authorities' early thinking on contact tracing

I have been unable to determine how the directive from the Ministry of Communications came to be, and whether it had been an early pit-stop on the way to a more detailed policy, or simply a regulatory cul-de-sac. One reading – buttressed by statements of the Minister and her staff – is that it was entirely an initiative of that department, with little involvement or prompting from their counterparts in the Ministry of Health. However, this research has determined that the health authorities leading South Africa's response to the virus had considered aggressive digital contact tracing from very early on.

The interest in a digitised contact-tracing approach was borne in part from recognition that cases could increase at a speed that 'manual' contact tracers can struggle to match, a point emphasised by various health officials interviewed for this research.

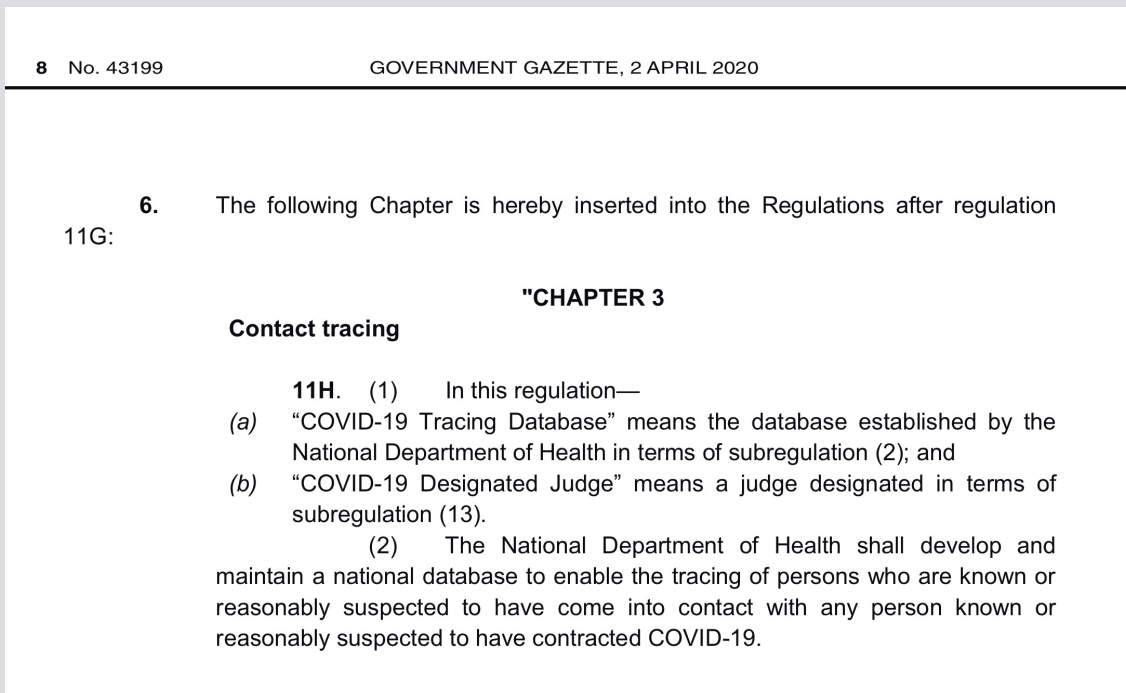
An advisor from the National Institute for Communicable Diseases suggested that South Africa's health authorities had expressed interest in digital contact tracing from the very early days of the pandemic, based on reported successes in China.

We had been aware at the NICD of the Chinese systems for contact tracing, which were the use of these mobile network operator data in order to track individuals. That had been widely publicised as a success story through news channels and the like...³⁰

The Minister of Health had convened a meeting in late March between health officials and senior representatives of Telkom and BCX, a Telkom subsidiary, to discuss development of a track-and-trace solution drawing on lessons from China – and this shaped South Africa's initial digital contact-tracing approach, which aimed to use locational information from mobile networks.

³⁰ Interview with Kerrigan McCarthy, National Institute for Communicable Diseases, on 28 September 2020.

Unpacking the April regulations



On 2 April 2020, the Minister of Cooperative Governance and Traditional Affairs published the policy framework for the state’s digital contact tracing regime – Regulation 11H (the ‘April regulations’). It was exactly four weeks after South Africa’s first confirmed infection, and also the same day that the count of confirmed Covid-19 cases in the country reached 1,462.

Regulation 11H outlined the process for gathering such information, and a variety of restrictions on its use, as well as oversight and transparency measures designed to protect against misuse and strike an appropriate balance between the right to privacy and the safeguarding of public health.³¹

The regulations provided for the establishment of a Covid-19 tracing database, where any relevant information gathered from communication networks would be stored, along with a

³¹ Government Gazette no 43199, 2 April 2020.

much wider array of information gathered by the National Department of Health to enable the tracing of people known to have tested positive for Covid-19 and contacts to whom they had been exposed. This database would include all information of patients tested in the public and private health sectors, including the names, addresses, identity numbers of everyone who is tested for Covid-19, including those who test negative.

The regulations vested the power in the Director General of Health to access users' locational information for contact tracing, by directing any 'electronic communications service provider'³² to hand over locational information about any person known or believed to have Covid-19, and anyone they have or are reasonably suspected to have come into contact with – exclusively for the purpose of contact tracing.

The regulations detailed several notable key privacy protections, including limiting how the powers could be used, by whom, and for how long, and they installed a judge to provide oversight, as well as various transparency measures, detailed below:

- **Limit on what the policy could be used for:** The regulations established a fairly strict purpose limitation for the use of communications data for contact tracing, in that the policy only allowed authorities to seek information relating to the location and movements of persons believed to have contracted or been exposed to the virus, and only for the purposes of 'addressing, preventing or combatting the spread of Covid-19 through the contact-tracing process.'³³ The information sought was not strictly limited to *locational* information (a broad reading of the regulation suggests that it might apply to other kinds of information from which location and movement could be inferred); however, the regulation expressly prohibits this contact-tracing process from being used to intercept the *content* of communication.³⁴ While South African law has been criticised for giving greater privacy protections to communication *content* on the faulty assumption that it is more sensitive than communication *metadata*,³⁵ the prohibition on intercepting content narrowed one possible way for the April contact-tracing regulation to be abused.
- **Limit on who may use the policy:** The fact that these powers were invested specifically in the health authorities could itself be seen as an important safeguard.

³² Under law this would include a range of industries, including internet service providers, fixed-line operators and mobile network operators; however, this research found that in design and implementation that policy was principally directed at mobile-network operators. Research on communications surveillance in South Africa often suggests that the state's interceptions capacity leans towards mobile telephony as well.

³³ Regulation 11H(11)b.

³⁴ Regulation 11H(12).

³⁵ Hunter, 'Cops and call records', 12-13.

Investing such powers in South Africa's security agencies may well have increased the risk of their abuse, both because of the notorious challenges for accountability and oversight of these structures,³⁶ and because of their existing prerogatives to intercept communication for law enforcement and intelligence purposes. The police and intelligence services clearly would have other work to which contact-tracing powers could be turned. But, that such a policy would exclude any role for South Africa's security agencies was by no means a given; as I discuss below, in early discussions officials assumed that the competence would fall to South Africa's law-enforcement or intelligence agencies – presumably because South Africa's interceptions legislation had already established a technical interface for data handovers from the mobile networks to these agencies. There was global precedent for this: in Israel, for example, the Shin Bhet security agency had already been enrolled in contact tracing using a controversial national-security interception tool.³⁷

- **Establishing special judicial oversight:** In a structure that echoed the 'RICA' oversight system, the regulations established a 'Covid-19 Designated Judge', appointed by the Minister of Justice, to receive a weekly report setting out the names and details of any person who is traced using this system. Thus, the regulations stopped short of giving the judge final authorisation in these decisions, but nonetheless provided oversight. The regulations also empowered the judge to make recommendations to ministers on amending the regulations, including to further protect privacy.³⁸
- **Establishing user notification:** The regulations provided that any person whose movements were traced in this system must be notified within six weeks of the end of the declared state of disaster. This represented a significant reversal of the state's position on user notification in communications surveillance: in the legal challenge to the state's surveillance law in the High Court and Constitutional Court in *amaBhungane*, various state bodies raised profound objections to this principle. While these agencies' main claim against user-notification in *amaBhungane* was that it would be self-defeating in security and policing contexts, officials have also been known to argue that post-surveillance notification would put an unacceptable logistical burden on the authorities.³⁹ The addition of user-notification in South Africa's proposed digital contact tracing was a notable safeguard in its own right, albeit subject to a delay, but also

³⁶ J Duncan, *The rise of the securocrats: The case of South Africa*. Johannesburg: Jacana Media, 2014, 114-118.

³⁷ Times of Israel, 'Shin Bet chief implores ministers not to renew coronavirus surveillance', 21 June 2020, <https://www.timesofisrael.com/shin-bet-chief-implores-ministers-not-to-renew-coronavirus-surveillance/>

³⁸ Regulation 11H(13)-(15).

³⁹ Hunter, 'Cops and call records', 29.

represented an evolution in the state's position since *amaBhungane* started working its way through the courts in 2017.

- **Establishing time limits and expiry date:** The regulations put time limits on the use of these powers. No request could be made about a person's movement reaching back earlier than March 2020 when the President declared a national state of disaster; any data that is collected as part of the contact-tracing process should be destroyed within six weeks if not needed for contact tracing; most importantly, the data-collection regulation itself would expire when the declared state of disaster lapses.⁴⁰ These provisions addressed a central concern arising from the global spread of Covid-19 emergency measures: that the emergency measures would outlast the emergency, and be turned to other purposes. The regulations did not require the outright destruction of the tracing database itself – which contains details of any persons who had been tested for Covid-19 and any information that was used for contact tracing. Rather, the regulation required that this database be stripped of any identifying information, and retained for public-health research going forward. The de-identification process must conform to any directions issued by the Covid-19 designated judge to protect the privacy of those whose information was collected.⁴¹
- **Other transparency measures:** As additional transparency measures, the regulations required that the Director General of Health and the designated judge must submit reports to Parliament on the shuttering of the contact-tracing system.

This framework earned cautious acknowledgement for its concessions to privacy,⁴² with some caveats – for example, surveillance scholar Jane Duncan noted that the judicial oversight of the system was limited to 'after the fact' scrutiny of tracking decisions, rather than the power to adjudicate tracking decisions before the fact, which is the common standard for judicial oversight in communications surveillance.⁴³ The fact that the policy called for some data from the tracing database to be de-identified and retained for research purposes raised concerns about the increasing potential for 'anonymous' datasets to be re-identified.⁴⁴ Others noted that certain safeguards could easily be improved – for example, by providing that people whose data was accessed through the regulation would

⁴⁰ Regulation 11(H)17.

⁴¹ Regulation 11(H)17.

⁴² D Milo & L Pillay, 'Tracing contacts by limiting privacy in the Covid-19 world: Constitutional or unlawful?' Daily Maverick, 8 April 2020, <https://www.dailymaverick.co.za/article/2020-04-08-tracing-contacts-by-limiting-privacy-in-the-covid-19-world-constitutional-or-unlawful/>

⁴³ J Duncan 'Covid-19, cellphone location tracking and SA's contradictory security response', Daily Maverick, 6 April 2020, <https://www.dailymaverick.co.za/article/2020-04-06-covid-19-cellphone-location-tracking-and-sas-contradictory-security-response/>

⁴⁴ M Hunter & C Thakur, 'Advocacy: New privacy rules for Covid-19 tracking a step in the right direction, but... ', News24, 4 April 2020, <https://www.news24.com/news24/Columnists/GuestColumn/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but-20200404-2>

be notified on an ongoing basis, rather than deferring notification to some distant endpoint when the pandemic might subside.⁴⁵

These caveats aside, these analyses seemed to agree that the regulations were a sign of seriousness on the part of the state to ensure that its digital contact-tracing efforts showed due regard for privacy, and would not be repurposed for other surveillance purposes. This sense of seriousness was underscored when the Minister of Justice named a particularly highly regarded jurist as the ‘designated Covid-19 judge’ who would oversee the digital contact-tracing system: former Constitutional Court justice Kate O’Regan.⁴⁶

Even then, it is hard to assess the safeguards and privacy protections in the April regulations purely on their own merits, or even on the signs of progress in the state’s views since *amaBhungane*. A key factor is that the privacy protections in the April regulations had by no means seemed a certain outcome, judged both by the spread of problematic Covid-19 surveillance programmes globally, and by the chaotic and ill-considered proposals being discussed within South African state structures leading up to the April regulations.

A senior figure in the process told me that the April regulations had only been developed after authorities had received legal advice that it would have been unlawful to try use RICA to track users’ locations for contact tracing. I could not establish whether authorities had made any interception requests under RICA before this happened. That the April approach would be focused only on telecommunications data was also no certain outcome: several sources told me that there was significant interest among policymakers to include banking data in the ‘track and trace’ policy, in an effort to replicate some of the reported interventions in South Korea. According to an advisor in the process, the Banking Association of South Africa had been involved in assessing the feasibility of this, but ultimately the executive rejected the proposal due to privacy concerns.

⁴⁵ A Gillwald and others, ‘Mobile phone data is useful in coronavirus battle. But are people protected enough?’, *The Conversation*, 27 April 2020, <https://theconversation.com/mobile-phone-data-is-useful-in-coronavirus-battle-but-are-people-protected-enough-136404>

⁴⁶ Statement by the Minister of Justice and Correctional Services, 3 April 2020, https://justice.gov.za/m_statements/2020/20200403-Covid-19-JusticeORegan.pdf

6

Abandoning the ‘location-tracking’ approach

By early May, Health officials were already shifting to develop new approaches to digital contact tracing, after realising that the location-tracking method was unfeasible. By mid May, requests for user location data from mobile networks had ceased, less than six weeks after the system had been announced – though this only emerged months later.

In late June, there were further amendments to the April contact-tracing regulations. Although there was no media release or statement to note or explain the amendments, they had the effect of shifting the purpose of the regulation from contact tracing to ‘geospatial hotspot mapping’, and to make provision for contact tracing through a mobile app.⁴⁷ According to the Covid-19 designated judge, these amendments followed a set of recommendations that she had tabled with cabinet ministers following her conclusion that the original objective of the contact-tracing regulations was unfeasible. Among those recommendations were that government should end the pursuit of contact tracing through mobile network data; that it should explore the use of aggregated network data for ‘hotspot’ mapping; that it should study the deployment of contact-tracing apps in other countries to assess the case for a South African app; and should undertake independent security audits of the systems it had set up.⁴⁸ (As it happens, the amendment regulations did not actually close off the potential to request users’ network data for contact tracing – a point I return to later.).

The Department of Health was slow to announce this change. In late April, the *Sunday Times* had reported that the ambitious digital contact-tracing system was still in development. While the Department had made requests to mobile network operators, it said it had not yet tracked any person, but a spokesperson projected confidence that the system was in development:

*‘We are finalising the data linkages to receive the information, and this is not fully operational as yet,’ health spokesperson Popo Maja told the Sunday Times. ‘We have been continuing with our current method of contact tracing until the IT system is fully functional.’ He said the development of the system is on schedule and that further information on the project will be made available when everything is in place.*⁴⁹

⁴⁷ Government Gazette no 43476, 25 June 2020.

⁴⁸ Interview with K O’Regan, Covid-19 Designated Judge, on 1 July 2020.

⁴⁹ Sunday Times, ‘Hi-tech system to trace Covid-19 contacts still being built’, 26 April 2020, <https://www.timeslive.co.za/sunday-times/news/2020-04-26-hi-tech-system-to-trace-covid-19--contacts---still-being-built/>

The Department of Health would not make further disclosures on its approach to digital contact tracing until mid-July, when National Department of Health policy official Milani Wolmarans appeared in a virtual hearing of the Western Cape provincial parliament. For several months the provincial Parliament's Covid-19 oversight committee had sought to get a representative from the National Department of Health to give a presentation on what was assumed to be an ongoing communications-surveillance programme. When Wolmarans finally appeared on 17 July, it was to tell the provincial committee that the department had long before ceased trying to use cellular location data for contact tracing:

Currently the National Department of Health is not involved in a digitised system that is a surveillance programme, in other words where we are monitoring the movement or location of any citizen in the country... There was an attempt to develop a system that would allow us to do that. However technical complexities and the privacy concerns around this and the protection around that had us move towards a more active-based contact-tracing service rather than a surveillance system using the data of the mobile network operators.⁵⁰

Wolmarans told the committee that data had only been sought from mobile networks under the contact-tracing programme from 17 April to 15 May 2020, and that all data collected in that period had subsequently had been destroyed.

Describing the programme as having merely been a 'proof of concept', Wolmarans outlined a range of problems that had made the programme unworkable. Firstly, she confirmed that cellular location data simply was not accurate enough for contact tracing, estimating that it could only pin-point a person within 50 to 200 metres, depending on the level of urbanisation and density of cellular towers.

Wolmarans added that in most instances the Department had not actually received locational information about people, only the physical address to which their SIM card was registered, which was sometimes inaccurate or out of date, telling the committee: 'There were a number of those where we found the address of the user of the phone and the RICA address were completely different, even in different towns.' (It should be noted that a Vodacom spokesperson told me the company had provided the Department with fairly detailed call-related data.⁵¹)

⁵⁰ Presentation by Milani Wolmarans, Ad-hoc committee on Covid-19, Western Cape Provincial Parliament, 17 July 2020. Video hearing available at: <https://www.youtube.com/watch?v=YMGBVLQgGZc>

⁵¹ An email from Vodacom spokesperson Byron Kennedy on 5 October 2020 said, 'Vodacom has provided the location data and date and time of calls made and received of COVID-19 positive subscribers to the Department of Health during the national state of disaster. This is the same historic call data (without the B party information, i.e. who the call was made to or received from) that we will normally provide to SAPS when we are served with a Section 205 Subpoena from the court.'

Wolmarans also pointed out that a device or phone number was found not always a reliable proxy for a person, telling the committee that ‘There are quite a number of individuals in South Africa that have up to five different phones that they are using.’ A similar set of assumptions had been criticised in ‘big data’ responses to the 2014-2016 Ebola outbreak.⁵²

Wolmarans did not say how many requests the Department had made to mobile network operators before it abandoned the approach. At the time of writing, it is still unclear how many requests were made, despite written requests to various officials in the Department of Health and telecoms industry. In late April, a spokesperson for Vodacom told the *Sunday Times* that it had provided data for 800 of its customers; this would have been just over a week after Wolmarans said the Department of Health started making such requests, on 17 April.⁵³ Of the other network operators, MTN reportedly declined to say how many requests it had received, and Cell C and Telkom did not respond to questions.

There is more to be said about the contact-tracing approaches that would follow, and there are lessons to be learned from the rapid development and quick conclusion to the approach first attempted through the April regulations.

⁵² S Erikson, ‘Cell phones & self and other problems with big data detection and containment during epidemics,’ *Medical Anthropology Quarterly*, 32, 3, 2018.

⁵³ *Sunday Times*, ‘Hi-tech system to trace Covid-19 contacts still being built’, 26 April 2020, <https://www.timeslive.co.za/sunday-times/news/2020-04-26-hi-tech-system-to-trace-covid-19-contacts---still-being-built/>

7

What went wrong?

Misunderstanding of the technology

At its heart, the policy appears to have been shaped by a dramatic over-estimation of the accuracy of the locational data available to mobile networks, and its usefulness for contact tracing.

Explaining the initial allure of the envisaged system, one health official said:

That was the great carrot that was dangling in front of us the whole time. We thought, if this works, then fantastic, because that would mean that you could enhance the effectiveness of contact tracing without any administrative overhead. So it was done with a lot of positive intent, but didn't work.⁵⁴

For the purposes of contact tracing, the National Institute for Communicable Diseases (NICD) initially defined a close contact as someone who has been within two metres of a Covid-19 positive person, or within a closed space with them.⁵⁵ The locational information from mobile networks simply lacks the granularity needed to pinpoint a person's location to that level of accuracy. In criminal investigations, researchers have used triangulation to get a more accurate picture of a person's precise location, but only long after the fact and using analysis of tower records which would not ordinarily be stored in a user's call records.⁵⁶ Leaving aside accuracy, locational data from a person's call records would only show the location of one party; a much wider data set would be needed to even begin to estimate who they might have been exposed to.

Misreading international responses

It is hard to overlook a fetishisation of high-tech responses to Covid-19 in international media, academic and policy circles. If it is true that South Africa's initial approach in digital contact tracing was modelled on an understanding of approaches in China, and

⁵⁴ Interview with Gaurang Tanna, NDoH, on 28 September 2020.

⁵⁵ National Institute for Communicable Diseases, Guidelines for COVID-19 Version 2.0, 8 March 2020.

⁵⁶ Interview with Jason Jordaan, DFIRLABS, on 10 January 2020.

an understanding that these were critical to successful containment of the pandemic, it is not at all clear that either understanding was correct. On the same day that South Africa published its first contact tracing regulations, 2 April, the *Financial Times* published a long-form article exploring the haphazard results borne by Chinese state surveillance in contact tracing in general, and in use of cellular data in particular:

While telecoms data has helped some local governments pin down potential coronavirus cases, there have been many problems with the information. Carriers track phone locations through the transmission towers to which users connect. The location data is not always accurate: depending on cell tower coverage, the estimated locations can be out by as much as 2 km.⁵⁷

Rather, the writers suggested, the most effective technological interventions in the outbreak had been the simplest, such as online medical questionnaires and health-checks when entering public spaces. This is to say nothing of the role of rapid testing capacity in China.⁵⁸

Limited external feedback

That the original policy was ill-conceived is not contested by those in Health. However, officials describe the decision-making process as being shaped by the understandable urgency of the moment, which allowed little room for delay or external input that may have identified incorrect assumptions or blindspots:

If we had just mapped out our data flow processes, and done some exploratory questioning around how feasible this idea is, we would have spent less time and energy on it, because we would have been reliably informed that this was not going to work. I think part of the reason we didn't do that was because there was so much momentum on this project. We had the brightest minds, capable programmers [in Telkom BCX], and they were itching to go... We didn't have the necessary perspective to stand back and think, well, what are we trying to do? And maybe that speaks to the oversight, the project conceptualization. But all of that is in the context of the immense pressure that we needed to do something today for our health services.⁵⁹

⁵⁷ Financial Times, 'China, coronavirus and surveillance: the messy reality of personal data', 2 April 2020.

⁵⁸ New York Times, 'Here's how Wuhan tested 6.5 million for coronavirus in days', 26 May 2020, <https://www.nytimes.com/2020/05/26/world/asia/coronavirus-wuhan-tests.html>

⁵⁹ Interview with Kerrigan McCarthy, National Institute for Communicable Diseases, on 2 November 2020

Missing fundamentals?

The accuracy and usefulness of the data sought in South Africa's first attempts at digital contact tracing may not be the only issue at stake. One provincial health official pointed to the understandably stretched capacity of the health services themselves as a huge limiting factor to any effective intervention, telling me: 'I can't go into the usefulness of the [mobile network] data, but the big question is what are we going to do with it? You need a squadron of data scientists, and very competent managers, to ask relevant questions of the data.'

Health authorities have been frank about the structural challenges facing many parts of South Africa's health system. While the causes for these are diverse, it may be that some of these challenges were always going to be an obstacle to any attempt to digitise or automate contact tracing in South Africa. For example, various delays in turning around testing results became a big problem for South Africa's health services, especially as Covid-19 cases surged.⁶⁰

With mounting cases, and test results regularly taking a week or more, one doctor who volunteered in a contact-tracing call centre in the early months of the pandemic told me contact tracing was 'like farting into a thunderstorm.' In May 2020, it was reported that patients were waiting up to ten days to get their test results.⁶¹ In June 2020, the national laboratory services told Parliament it was conducting about 15,000 tests a day, but had a backlog of over 70,000 samples, due in part to global test shortages.⁶² These significant challenges would surely hinder even a better-conceived digital contact-tracing approach.

⁶⁰ The modelling by Ferretti and others, 2020 (see n 5), suggested that after just three days' delay, notifying and isolating contacts of a person with Covid-19 does little to slow the spread of the virus.

⁶¹ Bhekisisa Centre for Health Journalism, 'National COVID-19 testing backlog means patients wait up to 10 days for results', 8 May 2020, <https://bhekisisa.org/health-news-south-africa/2020-05-08-south-africa-covid19-coronavirus-testing-national-backlog-nhls/>

⁶² National Health Laboratory Service, Presentation to Parliament's health committee, 10 June 2020, <https://pmg.org.za/committee-meeting/30439/>

8

What went right?

As a contact-tracing programme, the scheme devised in the April regulations was a failure. Yet its rapid abandonment could also be seen as a kind of success. Firstly, in the context of fears that health-surveillance powers would be re-purposed and abused, there is some comfort that health officials chose not to pursue a surveillance policy if it was not effective for the purpose it had been set up. Secondly, the decision to abandon and amend the contact-tracing policy is a credit to one of the safeguards written into the regulations – the oversight and recommendation power granted to the Covid-19 designated judge.

In an interview in July 2020, Justice Kate O'Regan confirmed that she had recommended an end to the attempt to use mobile location data for contact tracing, along with a range of other policy recommendations:

My advice to government was that at the current state of science, there is absolutely no suggestion that location data from cell phones will provide sufficiently accurate information for contact tracing, and that the regulation should be amended to make clear that the information obtained from mobile network operators will not be used for that purpose.⁶³

Justice O'Regan added that her other recommendations included the potential for aggregated network data to be used for 'hotspot' mapping; that government should do independent security audits of the systems it had established, and that it should study deployment of contact-tracing apps in other countries to assess the case for a South African app.

In considering the merits of the oversight role envisaged by the creation of a Covid-19 designated judge, O'Regan emphasised the importance of these recommendation powers, which she described as 'the meat of the role'. She argued that this forms part of an iterative approach to policy-making which is necessary in unprecedented crises.

⁶³ Interview with K O'Regan, Covid-19 Designated Judge, on 1 July 2020.

The recommendation power is important because this pandemic is unfolding very fast. And we are having to make policy in circumstances where the science is not yet ready. And so the only way to make policy in those circumstances is iteratively. As we keep learning, we keep reviewing and revising our policy and I think it's quite arguable that it is a duty in a pandemic. And the recommendation role allows a sort of independent engagement with the policy-making process around contact tracing and the use of digital technology to aid the combating of the disease. And in that way it's not very RICA-like.⁶⁴

While she was at pains not to express a view on the constitutionality of the Covid-19 regulations, O'Regan argued that the recommendation powers in the context of Covid-19 surveillance was a more important safeguard than the power to pre-authorise each tracking request. One of the early criticisms of the regulations was that it had fallen short of giving the Covid-19 designated judge the pre-authorisation powers that would be afforded to a judge overseeing interception of communications by police or intelligence agencies in RICA.⁶⁵ O'Regan argued that the unchanging circumstances of each contact-tracing request left limited scope for meaningfully adjudicating contact-tracing requests compared to the wide range of factors that might be adjudicated in an interception request for security or law enforcement purposes:

In circumstances where you're talking about whether you should permit the surveillance of a particular person, the conditions and circumstances of that particular person at that particular time are crucial to making that decision. When you're deciding in circumstance of a public health emergency whether you should know where a person with a particular disease is, the variability of that person's circumstances is entirely different.⁶⁶

Thus, although the contact-tracing system created through the regulations was unworkable, the recommendation powers created through the regulations paved the way for a shift in contact-tracing policies.

⁶⁴ Interview with K O'Regan.

⁶⁵ J Duncan, 'Staring down the securocrats', about:intel, 7 April 2020, <https://aboutintel.eu/covid-surveillance-south-africa/>

⁶⁶ Interview with K O'Regan.

Health officials involved in policy development described a similar need for an iterative approach in responding to the challenges of the pandemic. Said one:

We've had to think on our feet. We've had to think fast. We've had to think [about] effectiveness quickly, we've had to think [about] scale quickly. We were to think [about] a variety of contexts quickly. And I think all those made us take one or another decisions along the way. Initially, with COVID-19, contact tracing was fine... But we knew very soon we'll probably face a similar problem to other countries, and manual contact tracing will not keep up, and in fact, we already saw signs of it not keeping up early on in the pandemic. So we were always hunting for a solution that we could use to try shift some of the work we have to do onto technology. Early on, we tried out the mobile network operator data as the basis for contact tracing, and there were obviously technological issues, but there were legal issues and there were also privacy concerns. We had to figure out something else that was better and more enabling for the healthcare workers, enabling the patients and enabling the contacts of those patients, etc.⁶⁷

⁶⁷ Interview with Gaurang Tanna.

9

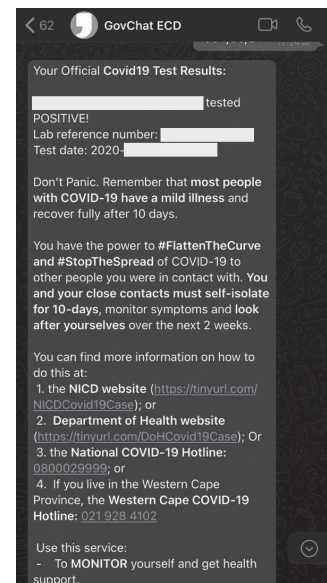
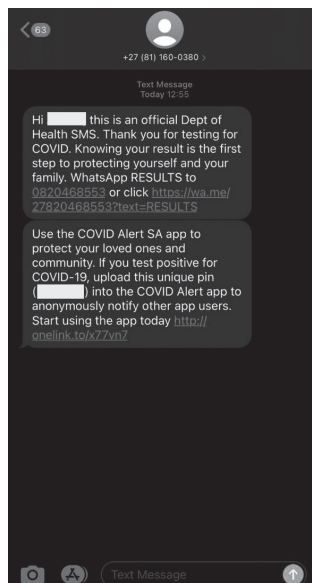
The shift to other approaches

Before the mobile network approach was even fully abandoned, the National Department of Health was already investigating other digital interventions for contact tracing – first, through a WhatsApp-SMS suite branded as CovidConnect, and more recently through the launch of the Covid Alert South Africa app. Separately, South Africa’s largest mobile network operator, Vodacom, began sharing aggregate data from its networks with several local and provincial government authorities, as well as the National Institute for Communicable Diseases and the Council for Scientific and Industrial Research (CSIR), a state-owned research and technology agency.⁶⁸

While each of these could be seen as a welcome move from the ill-considered first approach, it is troubling to note that each intervention was designed, and in some cases implemented, with no prior public announcement or consultation. While this can easily be understood as a result of the enormous burden on public health authorities, it may spell ill for public policy, and public trust.

CovidConnect

From early May, the National Department of Health started work on the messaging suite known as CovidConnect with a range of private sector providers, including GovChat, Telkom BCX, the Praekelt Foundation.



⁶⁸ Email from B Kennedy, Vodacom spokesperson, on 5 October 2020.

The CovidConnect platform uses a combination of WhatsApp and SMS interaction to invite users who receive a positive Covid-19 diagnosis to notify nominated contacts.⁶⁹ A person who undergoes a Covid-19 test receives a notification by SMS sent by Telkom BCX, directing the person to the GovChat WhatsApp bot channel in order to receive their result. There, they can also get further health support, and provide names and cell numbers of contacts whom they would like to receive an exposure notification. The nominated contacts are sent from GovChat back to Telkom BCX. Telkom BCX then sends an SMS to each nominated contact directing them to a Praekelt-hosted WhatsApp channel (HealthCheck) informing them of their possible exposure, and inviting them to monitor their health status for the next 14 days. Its relatively low-tech blend of SMS and WhatsApp interaction are a design response to South Africa's high uptake of WhatsApp, and restrictions on 'broadcast' using WhatsApp Business API. For users without a smartphone, the platform does make it possible to obtain their result from another WhatsApp cell number; officials also plan to roll out USSD channels to support access to results for people without smartphones.⁷⁰

The Minister of Health publicly announced the launch of CovidConnect in mid-July 2020,⁷¹ but only after an initial pilot phase in the Western Cape, and rollout in all provinces.⁷²

The Department of Health's Gaurang Tanna explained that these tools were never meant to replace the work of manual contact-tracing, which is largely managed through provincial health departments. 'This was never meant to replace, it was always meant to complement what they did, because we knew there would be in many scenarios where CovidConnect would not be sufficient.' He estimated that the number of users who obtain their results via CovidConnect amounts to 22% of total cases, with fewer using the contact-tracing feature.⁷³

The Bluetooth app

In September 2020, the Minister of Health announced the launch of the Covid Alert South Africa app, which was developed pro bono by Discovery Health using the Google-Apple exposure notification protocol.⁷⁴ Google and Apple released the protocol in April 2020 as

69 Spotlight, 'COVID-19: The trial and error of digital contact tracing in SA', 28 July 2020, <https://www.spottlightnsp.co.za/2020/07/28/covid-19-the-trial-and-error-of-digital-contact-tracing-in-sa/>

70 Interview with Gaurang Tanna, National Department of Health, on 28 September 2020.

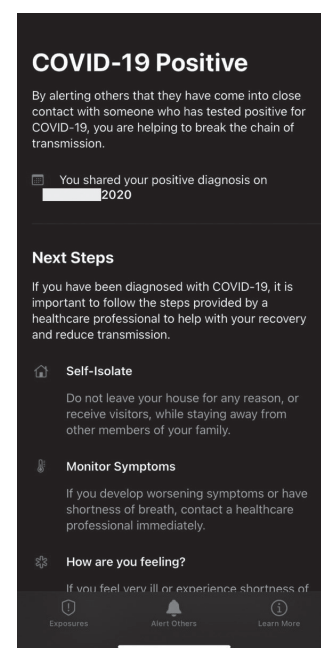
71 Statement by Minister of Health, 17 July 2020, <https://sacoronavirus.co.za/2020/07/17/health-department-launches-covid-service-portal/>

72 Presentation by Wolmarans, 17 July 2020.

73 Interview with Gaurang Tanna, on 28 September 2020.

74 Minister of Health, 1 September 2020, <https://sacoronavirus.co.za/2020/09/01/department-of-health-launches-powerful-new-tool-to-strengthen-covid-19-contact-tracing/>

a privacy-preserving response to efforts by governments and a host of technology firms to develop contact-tracing apps. It works by allowing smartphones to exchange random proximity IDs over Bluetooth and create an anonymous, temporary record of proximity with other devices; if a user has a confirmed Covid-19 case, the app can send an anonymous alert to other devices that registered close proximity in the preceding 14 days. In doing so, the app creates a framework for users to notify their contacts of exposure to the virus, while sidestepping some of the major privacy risks with other digitised approaches: use of the app is voluntary, and it does not collect information about a user's location or contacts.⁷⁵ Thus, the Covid Alert app appears not to revive the same searching questions on privacy protection of the government's first approaches to contact tracing, although its reliance on digital inclusion in the South African context raises questions about its efficacy.⁷⁶ A study of equivalent apps in Europe found that they were 'generally well-behaved from a privacy point of view' but did result in user and device data being collected by Google servers.⁷⁷ This points to the need for further research on the underlying security and data collection components of the South African app, a need potentially complicated by the fact that its source code has not been published, unlike most international equivalents.⁷⁸



Aggregate mobile data

The amendment to contact-tracing regulations on 26 June 2020 made provision for the Department of Health to access to mobile data for 'geospatial hotspot mapping'. In fact, at least one network operator had already been sharing aggregate data with certain public bodies for at least a month – Vodacom.

According to a Vodacom spokesperson, the company is sharing aggregated data with the NICD, the CSIR, the Free State Department of Health, the Eastern Cape Provincial Department of Health, and the City of Cape Town.

⁷⁵ Google & Apple, Exposure Notifications: Using technology to help public health authorities fight COVID-19, n.d. <https://www.google.com/Covid19/exposurenotifications/>
⁷⁶ Research ICT Africa, 'Contact tracing in South Africa, Policy Brief 4, September 2020, <https://researchictafrica.net/wp/wp-content/uploads/2020/09/RIA-Policy-Brief-Contact-Tracing-Sep2020.pdf>
⁷⁷ Privacy International, 'Study finds gaps in GAEN contact tracing apps privacy protection', n.d., <https://privacyinternational.org/examples/4189/study-finds-gaps-gaen-contact-tracing-apps-privacy-protection>
⁷⁸ XDA News, List of the countries using Google and Apple's COVID-19 Contact Tracing API, n.d., <https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/>

*Vodacom has provided aggregated data to the South African government to assist with tracking and tracing the spread of the virus. This includes mobility analytics at a ward level related to the lockdown and population movements for disease spread modelling at a ward and district level... Sharing of anonymised aggregated data is through a dedicated secure dashboard and a data sharing portal.*⁷⁹

Similar arrangements have appeared between network operators and health authorities in a number of other countries over the course of the year.⁸⁰

According to one official with access to the system, the interface gives officials insight into how many devices are connected to a particular part of Vodacom's network at any given time, by providing a simple count of the devices without any identifying information about the devices themselves.

One dataset in the interface gives a simple count of unique devices connected in a particular area – in other words, giving insight into population density. A second dataset shows a count of the total number of unique devices leaving one part of the network and arriving at another, which gives insight into population movements and commuter patterns. These datasets were reportedly used to guide modelling for Covid-19 in South Africa,⁸¹ but could also be used to monitor compliance with lockdown conditions.

The CSIR's Information and Cyber Security Centre has used Vodacom's aggregate network data for a 'COVID-19 Tracker' project that models population mobility, which the agency said could be used to help health administrators identify potential hotspots, and allocate resources or issue alerts in particular areas. It added that the CSIR saw applications for the system beyond Covid-19, including crime prevention.⁸² The same unit within the CSIR is carrying out Covid-19 'hotspot mapping' for the National Department of Health; while it has been reported that this mapping service uses aggregate data from mobile networks showing population movement, in addition to approximate location of positive Covid19 cases from the National Institute for Communicable Diseases,⁸³ this appears not to be the case. According to a CSIR manager of the project, the hotspot mapping does not use network data at all, only data on the locations of Covid-19 cases from the NICD, which is approximated in order to protect the anonymity of individual patients.⁸⁴

⁷⁹ Email from B Kennedy, Vodacom spokesperson, on 5 October 2020.

⁸⁰ Privacy International, Tracking the global response to Covid-19, <https://privacyinternational.org/examples/tracking-global-response-covid-19>

⁸¹ Interview with S Silal, MASHA, on 11 July 2020.

⁸² CSIR media release, 30 June 2020, <https://www.csir.co.za/tracking-mobility-better-understand-covid-19>

⁸³ See D Johnson, 'Assessment of contact tracing options for South Africa,' Research ICT Africa, October 2020, 20, <https://researchictafrica.net/publication/assessment-of-contact-tracing-apps-for-south-africa/>

⁸⁴ Email from Dr Jabu Mtsweni, CSIR, on 2 November 2020.

10

Further problems with the regulations

Before turning to the lessons to be drawn from the unfolding events around South Africa's digital contact-tracing approaches, it is necessary to outline a few remaining problems with the contact-tracing regulations. It has already been noted that, although the Department of Health has by all accounts stopped seeking users' mobile-network location data for contact tracing, the 26 June amendments to the regulations actually left these powers intact. The amendment also appears to have expanded the purpose of the database that had been created through the regulations in 2 April.

Keeping mobile network contact tracing 'on the books'


The 2 April regulation stipulated that mobile location data '... 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.'

As detailed earlier, the 26 June amendment followed recommendations from the Covid-19 designated judge that cell phone location data cannot be used for contact tracing, but that anonymised network data could potentially be used for mapping pandemic 'hotspots'. However, the amended regulations simply expanded the grounds for which the Department of Health could access mobile data 'when necessary for the purposes of addressing, preventing or combatting the spread of COVID-19 through the contact tracing process or geospatial hotspot mapping' [emphasis added].⁸⁵

⁸⁵ Regulation 8(11)b, per Government Gazette no 43476.

April 2020

(2) The National Department of Health shall develop and maintain a national database 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.



"(2) The National Department of Health shall develop and maintain a national database in order to guide appropriate responses in addressing, preventing or combatting the spread of COVID-19, including contact tracing and geospatial hotspot mapping.";

June 2020

The decision to retain this contact-tracing power, at least on paper, is difficult to justify, not least of all since the authorities have emphasised their desire to limit risks to privacy. All parties involved seem to agree that mobile data is effectively useless for contact tracing, and the 26 June amendment appeared to be a good-faith acknowledgement that the initial policy was misconceived. It is also unclear that individuals' mobile location data is necessary for the purpose of hotspot mapping; while aggregated network data as provided by Vodacom can be used to map population density, the approximate location of individual Covid-19 cases could arguably be drawn from residential information that is collected as a matter of course when a person undergoes a test for Covid-19, or simply deduced from the location where a positive test sample was collected. At the very least, if a person's mobile location data is necessary for hotspot mapping, nobody appears to have made that case publicly in South Africa.

Expanding the purpose for data collection

The amendment of 26 June also expanded the purpose for collection and storage of people's personal information during the pandemic. The 2 April regulations provided for the National Department of Health to establish a 'Covid-19 Tracing Database,' to store a range of personal information about people who get tested for Covid-19, and people who are known or suspected to have been exposed to the virus. The regulation gave this database a very clear and limited purpose: to 'enable the tracing of persons' with Covid-19.⁸⁶ The 26 June amendment effectively repurposed this database, renaming it

⁸⁶ Regulation 11(H)c, per Government Gazette no 43199.

‘the Covid-19 Database’, and expanding its purpose to ‘*guid[ing] appropriate responses in addressing, preventing or combatting the spread of Covid-19, including contact tracing and geospatial hotspot mapping [emphasis added].*’⁸⁷ In other words, the database could serve any purpose deemed necessary to guiding policy responses to Covid-19.

April 2020

(11) The information referred to in subregulation (10)—

- (a) may only be obtained in relation to the location or movements of persons during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated;
- (b) may only be obtained, used or disclosed by authorised persons and 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;



“(b) may only be obtained, used or disclosed by authorised persons and 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 or geospatial hotspot mapping;”

June 2020

Again, this amendment appears to have been handed down without explanation. There may well be an underlying public-health imperative for expanding the purpose of centralised collection of data about people exposed to the virus, which may outweigh the data protection risks, but the public case has yet to be made.

One explanation given for some of these ‘loose ends’ is that they are also a product of iterative policymaking. The official leading the development of the Department of Health’s digital platforms said the regulations were amended at a time when CovidConnect and CovidAlert had yet to be implemented at scale, while their regulatory needs were still unclear: ‘It was important to future proof legislation in case we needed to move beyond the envisaged methods. The evolution of contact tracing was through learning from implementation.’⁸⁸

⁸⁷ Regulation 8(2), per Government Gazette no 43476.

⁸⁸ Email from G Tanna, on 3 November 2020.

11

The lessons for privacy

This research, while critical of its findings, does not presume to downplay the seriousness of the public-health challenges of the Covid-19 pandemic, nor the significant efforts of South Africa's health authorities and healthcare workers to meet those challenges. Nor does it mean to suggest that any missteps in digital contact tracing were unique to South Africa. Quite the opposite.

In addition to the catastrophic impact of the global coronavirus pandemic on health and economic well-being, it seems to be generally agreed that has been bad for privacy. Certainly, across the world, the digitisation of many parts of public life, the scramble for high-tech tools for screening, contact tracing and quarantine enforcement, and the gathering and centralisation of huge amounts of health data, have presented very many challenges for data protection. The sheer urgency of the pandemic has resulted in a wide range of technological interventions based on assumptions that may be untested, and where the results have yet to be fully evaluated.

In many respects, the South African case has followed this line. Its first approaches to contact tracing were poorly designed, based on false assumptions, and fuelled by an understandable sense of panic, and they resulted in unnecessary intrusions on data protection principles. The later approaches seem more carefully considered, but have often been designed and implemented unilaterally, without public consultation or scrutiny. While the good intentions underpinning these interventions is undeniable, there is a lack of public information about the workings and performance of these systems outside of press releases and promotional campaigns, and limited opportunity for public debate about their merits.

This in part reflects a troubling absence from key oversight bodies. Parliament's health committee held just eight meetings on the government's Covid-19 response in the first eight months of the pandemic.⁸⁹ On the data protection elements of the pandemic, South Africa's nascent data authority, the Information Regulator, issued a brief guidance note in

⁸⁹ The committee did hold a range of other meetings through the year on non-Covid19 matters, such as reviews of departmental budgets and performance plans, and briefings on the National Health Insurance plan. Parliamentary Monitoring Group website, Portfolio Committee on Health: <https://pmg.org.za/committee/63/>

April to affirm that it considered the use of mobile data for contact tracing to be lawful,⁹⁰ but otherwise appears to have been largely disengaged from these events.

This research has stopped short of making a finding on the efficacy and impact of the approaches to digital contact tracing that evolved from the shift away from mobile location data in South Africa. It remains an unresolved question – and not only in South Africa. The WHO, in recognising the potential for digital contact tracing systems in Covid-19, has noted there is limited understanding of their impact. A review of 15 studies on contact tracing systems, for both Covid-19 and other diseases, found no empirical evidence of the benefit of automated contact-tracing, and some studies with evidence that partly automated contact-tracing systems could result in better data collection and response rates compared to manual contact-tracing, but no research to measure any effect on Covid-19 transmission.⁹¹

Public health officials have responded to scepticism about the potential efficacy of CovidConnect and Covid Alert platforms by arguing that every bit helps. Said one: ‘We have to approach things in a multimodal way, because our reach is then better. No system is universally effective, but some collective input of many systems may help.’⁹²

In a media interview, the Department of Health’s Gaurang Tanna made a similar point:

‘People say the [Covid Alert] app is not perfect. I’ve studied hundreds of contact tracing solutions globally and I’ve not come up with one perfect solution. There is no panacea in digital contact tracing... Every 100 infections we avert with this technology we save two lives. And those two lives do matter. It’s a fairly low-cost intervention and it’s the least South Africans can do to help us fight Covid-19.’⁹³

Certainly, more research is needed, and more information about the targets and outcomes of each intervention.

One risk of an approach rooted in technological determinism is that it leaves little room for pause, consultation and contestation. The realisation that human rights requires careful

⁹⁰ Information Regulator, ‘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,’ 3 April 2020, <https://justice.gov.za/infocreg/docs/infocregsa-guidancenote-ppi-covid19-20200403.pdf>

⁹¹ Isobel Braithwaite and others, ‘Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19’, *The Lancet Digital Health*, 2, 11, 19 August 2020, [https://doi.org/10.1016/S2589-7500\(20\)30184-9](https://doi.org/10.1016/S2589-7500(20)30184-9)

⁹² Interview with Kerrigan McCarthy, NICD, on 5 November 2020.

⁹³ Daily Maverick, ‘COVID Alert SA app: The fine balance between public health, privacy and the power of the people’, 13 October 2020, <https://www.dailymaverick.co.za/article/2020-10-13-covid-alert-sa-app-the-fine-balance-between-public-health-privacy-and-the-power-of-the-people/>

protection in times of rapid technological change pre-dates the Covid-19 era⁹⁴ – yet it is surely just as true now.

Aside from the risks to privacy and other digital rights, there may be unknown opportunity costs when policy processes are driven by a fixation on technological solutions. As medical anthropologist Susan Erikson wrote in a scathing review of tech-driven responses to the West Africa ebola outbreaks of the 2010s, ‘In medical humanitarian crises, there is always the chance that new technologies will forestall more fundamental and essential steps and strategies of health crisis management.’⁹⁵

It is unclear what opportunity costs may have come from any misadventures in South Africa’s initial attempts at digital contact tracing. It may be that the time and resources put towards the pursuit of the proposed system could have been spent more effectively elsewhere, although this idea was disputed by the public-health officials interviewed for this research. It may also be that missteps throughout the rollout of digital strategies – policy failures, lack of deliberation or consultation, and miscommunication and lack of information – depleted another finite resource: public trust. Months later, fears about privacy and misinformation about government tracking appear to be barriers to uptake of the Covid Alert app.⁹⁶ It cannot be said with certainty that past errors in South Africa’s Covid-19 response are a significant cause of these fears, but they probably did not help.

Nevertheless, if the global narrative of privacy in a pandemic is that the crisis will spark emergency powers that are only ever excessive, expansive and ever-lasting, the South African case did not quite fit.

⁹⁴ See K O’Regan, ‘Public law, the digital world and human rights: Challenges ahead’, *Judicial Review*, 25, 1, 2020, DOI: 10.1080/10854681.2020.1732742

⁹⁵ Erikson, 2018, 333.

⁹⁶ Daily Maverick, ‘COVID Alert SA app: The fine balance between public health, privacy and the power of the people’, 13 October 2020, <https://www.dailymaverick.co.za/article/2020-10-13-covid-alert-sa-app-the-fine-balance-between-public-health-privacy-and-the-power-of-the-people/>

12

Recommendations

As doomed as the policy may have been, the privacy protections in the April regulations suggested the work of a government, or at least public servants within it, both willing and capable of thinking creatively and progressively about data protection and surveillance reform, even in a time of crisis. It is remarkable to think that in the time of an unprecedented global pandemic, and in the course of just a few days, the state was able to produce a policy framework that moved the water mark for surveillance oversight in South Africa, adopting positions that the Ministers of Police and State Security had fought against in RICA litigation just weeks before. As much as this is a credit to the officials involved, it is also a development that appears to have been shaped by years of activism, advocacy and litigation towards surveillance reform. At the time of writing, the Constitutional Court's judgment in *amaBhungane* was still pending, with no certainty that it would rule in favour of the applicants. Yet in those April regulations, a small *amaBhungane* victory could already be found.

However, the policies described here were passed as emergency regulations in March 2020, for a national state of disaster that was initially to last only three months. The Covid-19 pandemic has proved to be lasting; it is past time to revisit and reassess these short-term policies.

The Covid-19 era is sure to generate many lessons and cautionary tales for technological responses to future crises. But this research has flagged the need for shorter-term interventions to be applied to the current moment. These include that:

- Parliament should initiate as a matter of urgency a public and participatory review of the regulations pertaining to contact tracing and the Covid-19 database;
- In the meantime, the power to access mobile location data using these regulations should be removed from the policy immediately, and all users whose data was accessed using this mechanism must be notified promptly;
- The National Department of Health should release full and detailed reporting on the design, implementation, and impact of each component of South Africa's Covid-19

digital health responses, including the initial use of mobile network data, CovidConnect and Covid Alert, and use of aggregated network data. This should include details of data-sharing agreements with all parties involved in the systems, key performance indicators for the systems, and costs incurred in the development and maintenance of each system;

- The Department should commission independent security audits of each of these systems, and publish the findings with speed;
- In recognition that there is still inadequate oversight of data protection questions at large, that the Information Regulator should work urgently to address its remaining capacity gaps, and develop a public plan for how it will take stewardship of Covid-19 data protection questions in 2021.

It is commonly said that those living through the Covid-19 era must adjust to a ‘new normal’. Perhaps so. But it is vital that this new normal is shaped by basic democratic principles of transparency, public participation, accountability, and protection for human rights – including, in this case, privacy and data protection.

- Access Now, Recommendations on privacy and data protection in the fight against COVID-19, March 2020, <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>
- African Commission on Human and Peoples' Rights, Declaration of principles of freedom of expression and access to information in Africa, 2019.
- amaBhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others* CCT 278/19.
- amaBhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others* (25978/2017) [2019] ZAGPPHC 384 [2019].
- Bhekisisa Centre for Health Journalism, 'Can you pause a pandemic? Inside the race to stop the spread of COVID-19 in South Africa', 26 March 2020, <https://bhekisisa.org/features/2020-03-26-can-you-pause-a-pandemic-inside-the-race-to-stop-the-spread-of-covid19-in-south-africa/>
- Bhekisisa Centre for Health Journalism, 'National COVID-19 testing backlog means patients wait up to 10 days for results', 8 May 2020, <https://bhekisisa.org/health-news-south-africa/2020-05-08-south-africa-covid19-coronavirus-testing-national-backlog-nhls/>
- A Blumberg & P Eckersley, 'On locational privacy, and how to avoid losing it forever', White Paper, Electronic Frontier Foundation, 2009, <https://www.eff.org/files/eff-locational-privacy.pdf>
- I Braithwaite and others, 'Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19', *The Lancet Digital Health*, 2, 11, 19 August 2020, [https://doi.org/10.1016/S2589-7500\(20\)30184-9](https://doi.org/10.1016/S2589-7500(20)30184-9)
- Daily Maverick*, 'Common cellphone tracking service used in ambush and murder of top policeman Kinnear', 23 September 2020, <https://www.dailymaverick.co.za/article/2020-09-23-common-cellphone-tracking-service-used-in-ambush-and-murder-of-top-policeman-kinnear/>
- Daily Maverick*, 'COVID Alert SA app: The fine balance between public health, privacy and the power of the people', 13 October 2020, <https://www.dailymaverick.co.za/article/2020-10-13-covid-alert-sa-app-the-fine-balance-between-public-health-privacy-and-the-power-of-the-people/>
- J Duncan. *The rise of the seurocrats: The case of South Africa*. Johannesburg: Jacana Media, 2014.
- J Duncan, *Stopping the spies: Constructing and resisting the surveillance state in South Africa*. Johannesburg: Wits University Press, 2018

- J Duncan, 'Covid-19, cellphone location tracking and SA's contradictory security response' *Daily Maverick*, 6 April 2020, <https://www.dailymaverick.co.za/article/2020-04-06-covid-19-cellphone-location-tracking-and-sas-contradictory-security-response/>
- J Duncan, 'Staring down the securocrats', about:intel, 7 April 2020, <https://aboutintel.eu/covid-surveillance-south-africa/>
- S Erikson, 'Cell phones & self and other problems with big data detection and containment during epidemics,' *Medical Anthropology Quarterly*, 32, 3, 2018.
- L Ferretti and others, 'Quantifying SARS-onmission suggests epidemic control with digital contact tracing', *Science*, 368, 6491, 8 May 2020. DOI: 10.1126/science.abb6936
- Financial Times*, 'China, coronavirus and surveillance: The messy reality of personal data', 2 April 2020.
- U Gasser and others, 'Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid', *Lancet Digital Health*, 2, 29 June 2020, [https://doi.org/10.1016/S2589-7500\(20\)30137-0](https://doi.org/10.1016/S2589-7500(20)30137-0)
- A Gillwald and others, 'Mobile phone data is useful in coronavirus battle. But are people protected enough?' *The Conversation*, 27 April 2020, <https://theconversation.com/mobile-phone-data-is-useful-in-coronavirus-battle-but-are-people-protected-enough-136404>
- Google & Apple, 'Exposure notifications: Using technology to help public health authorities fight COVID-19', 2020, <https://www.google.com/Covid-19/exposurenotifications/>
- M Hunter 'Cops and call records: Policing and metadata privacy in South Africa', Media Policy and Democracy Project, 2020, <https://mediaanddemocracy.com/>
- M Hunter, 'Open letter to Bheki Cele, RICA victim', *News24*, 25 February 2020, <https://www.news24.com/news24/Columnists/GuestColumn/open-letter-to-bheki-cele-rica-victim-20200225>
- M Hunter, 'Digital privacy in the time of pandemics,' *amaBhungane*, 31 March 2020, <https://amabhungane.org/advocacy/advocacy-comment-digital-privacy-in-the-time-of-pandemics/>
- M Hunter & C Thakur, 'Advocacy: New privacy rules for Covid-19 tracking a step in the right direction, but...' *News24*, 4 April 2020, <https://www.news24.com/news24/Columnists/GuestColumn/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but-20200404-2>
- IOL*, 'Coronavirus in SA: WHO boss praises South Africa's response to Covid-19 pandemic', 1 April 2020, <https://www.iol.co.za/news/politics/coronavirus-in-sa-who-boss-praises-south-africas-response-to-covid-19-pandemic-45923836>
- Information Regulator, '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,' 3 April 2020, <https://justice.gov.za/inforeg/docs/inforegsa-guidancenote-ppi-covid19-20200403.pdf>
- The International Principles on the Application of Human Rights to Communications Surveillance, 2014, <https://necessaryandproportionate.org/>

- D Johnson, 'Assessment of contact tracing options for South Africa,' Research ICT Africa, October 2020, 20, <https://researchictafrica.net/publication/assessment-of-contact-tracing-apps-for-south-africa/>
- D Lyon, 'The coronavirus pandemic highlights the need for a surveillance debate beyond 'privacy'', *The Conversation*, May 2020, <https://theconversation.com/the-coronavirus-pandemic-highlights-the-need-for-a-surveillance-debate-beyond-privacy-137060>
- D Milo & L Pillay, 'Tracing contacts by limiting privacy in the Covid-19 world: Constitutional or unlawful?' *Daily Maverick*, 8 April 2020, <https://www.dailymaverick.co.za/article/2020-04-08-tracing-contacts-by-limiting-privacy-in-the-covid-19-world-constitutional-or-unlawful/>
- Minister of Communications and Digital Technology, Directions, GN 417, 26 March 2020.
- Minister of Health, 17 July 2020, <https://sacoronavirus.co.za/2020/07/17/health-department-launches-covid-service-portal/>
- Minister of Health, 1 September 2020, <https://sacoronavirus.co.za/2020/09/01/department-of-health-launches-powerful-new-tool-to-strengthen-covid-19-contact-tracing/>
- Minister of Justice and Correctional Services, 3 April 2020, https://justice.gov.za/m_statements/2020/20200403-Covid-19-JusticeORegan.pdf
- National Institute for Communicable Diseases, Guidelines for COVID-19 Version 2.0, 8 March 2020.
- National Health Laboratory Service, Presentation to Parliament's health committee, 10 June 2020, <https://pmg.org.za/committee-meeting/30439/>
- New Frame editorial, 'South Africa faces a stark political choice', 29 May 2020, <https://www.newframe.com/south-africa-faces-a-stark-political-choice/>
- New York Times*, 'Here's how Wuhan tested 6.5 million for coronavirus in days', 26 May 2020, <https://www.nytimes.com/2020/05/26/world/asia/coronavirus-wuhan-tests.html>
- K O'Regan, 2020, Public law, the digital world and human rights: Challenges ahead, *Judicial Review*, 25, 1, 2020, DOI: 10.1080/10854681.2020.1732742
- Presidency of the Republic of South Africa, High-Level Review Panel Report on the State Security Agency', December 2018, <http://www.thepresidency.gov.za/download/file/fid/1518>
- Privacy International, 'Location data and Covid-19', n.d., <https://privacyinternational.org/examples/location-data-and-covid-19>
- Privacy International, 'Study finds gaps in GAEN contact tracing apps privacy protection', n.d., <https://privacyinternational.org/examples/4189/study-finds-gaps-gaen-contact-tracing-apps-privacy-protection>
- Research ICT Africa, 'Contact tracing in South Africa, Policy Brief 4', September 2020, <https://researchictafrica.net/wp/wp-content/uploads/2020/09/RIA-Policy-Brief-Contact-Tracing-Sep2020.pdf>

- A Singh & M Power, 'New digital regulations mean the state can track you – no questions asked,' *Mail & Guardian*, 31 March 2020, <https://mg.co.za/article/2020-03-31-new-digital-regulations-mean-the-state-can-track-you-no-questions-asked/>
- Spotlight*, 'COVID-19: The trial and error of digital contact tracing in SA', 28 July 2020, <https://www.spotlightnsp.co.za/2020/07/28/covid-19-the-trial-and-error-of-digital-contact-tracing-in-sa/>
- Sunday Times*, 'Hi-tech system to trace Covid-19 contacts still being built', 26 April 2020, <https://www.timeslive.co.za/sunday-times/news/2020-04-26-hi-tech-system-to-trace-covid-19--contacts---still-being-built/>
- Times of Israel*, 'Shin Bet chief implores ministers not to renew coronavirus surveillance', 21 June 2020, <https://www.timesofisrael.com/shin-bet-chief-implores-ministers-not-to-renew-coronavirus-surveillance/>
- UN Office of the High Commissioner on Human Rights, 'COVID-19: States should not abuse emergency measures to suppress human rights – UN experts', 16 March 2020, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E>
- Viewfinder, 'Details of two additional alleged lockdown killings by police revealed', 30 April 2020, <http://viewfinder.org.za/details-of-two-additional-alleged-lockdown-killings-by-police-revealed/>
- S Whitelaw and others, 'Applications of digital technology in COVID-19 pandemic planning and response', *Lancet Digital Health*, 2, 29 June 2020, [https://doi.org/10.1016/S2589-7500\(20\)30142-4](https://doi.org/10.1016/S2589-7500(20)30142-4)
- World Health Organisation, 'Contact tracing in the context of COVID-19: interim guidance', 10 May 2020, <https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19>
- World Health Organisation, 'Digital tools for COVID-19 contact tracing', 2 June 2020, https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1
- XDA News, List of the countries using Google and Apple's COVID-19 Contact Tracing API, n.d, <https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/>

Media Policy and Democracy Project

The Media Policy and Democracy Project (MPDP) was launched in 2012 and is a joint collaborative research project between the Department of Communication Science at the University of South Africa (UNISA), and Department of Journalism, Film and Television at the University of Johannesburg (UJ). The MPDP aims to promote participatory media and communications policymaking in the public interest in South Africa.

Visit mediaanddemocracy.com for more information.

This report was supported by a grant from the Open Society Foundation for South Africa (OSF-SA)



**OPEN SOCIETY FOUNDATION
FOR SOUTH AFRICA**