A South African Public Law Perspective on Digitalisation in the Health Sector

Digital Pathways Paper Series
DOI: https://doi.org/10.35489/BSG-DP-WP_2021/05

Prof. Firoz Cachalia and Prof. Jonathan Klaaren

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD

Digital Pathways at Oxford

Prof. Firoz Cachalia, *University of the Witwatersrand* and Prof. Jonathan Klaaren, *University of the Witwatersrand*

Paper 15
July 2021

Digital Pathways at Oxford is a research programme based at the Blavatnik School of Government, University of Oxford. It produces cutting-edge research across the fields of public policy, law, economics, computer science, and political science to support informed decision-making on the governance of digital technologies, with a focus on low- and middle-income countries.

This paper is part of a series of papers on technology policy and regulation, bringing together evidence, ideas and novel research on the strengths and weaknesses of emerging practice in developing nations. The views and positions expressed in this paper are those of the author and do not represent the University of Oxford.

Citation:
Cachalia, F. & Klaaren, J. (2021). *A South African Public Law Perspective on Digitalisation in the Health Sector*. Digital Pathways at Oxford Paper Series; no. 15. Oxford, United Kingdom

https://www.bsg.ox.ac.uk/research/research-programmes/digital-pathways

@DigiPathOxf
Cover image: © Shutterstock / Richie Satnam

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

Digital Pathways at Oxford

Our future is a race between the growing power of our technology and the wisdom with which we use it. Let's make sure wisdom wins.
Stephen Hawking

Table of Contents

Part One: Introduction *2*

Part Two: The Health Sector in South Africa – a Regulatory Overview from a Public Law Perspective *5*

Part Three: Digital Health Interventions in South Africa *8*

- Health clients *8*
- Healthcare providers *9*
- Health system or resource managers *10*
- Data services *11*

Part Four: The COVID-19 Tracing Database and subsequent technological initiatives to enhance digital contact tracing in South Africa *13*

Part Five: Conclusion *16*

Part One: Introduction

The impact of digitalisation on society has posed and re-posed a number of significant questions: What should be the limits of information stored by the government of its citizens? How can that information be appropriately shared with persons and firms in the private sector in order to unlock its economic value? Why does it seem as if the technology changes faster than the law can respond? What rights does an individual have in the information about that individual?

We explored some of the questions posed by digitalisation in an accompanying working paper focused on constitutional theory: *Digitalisation, the 'Fourth Industrial Revolution' and the Constitutional Law of Privacy in South Africa*. In that paper, we asked what legal resources are available in the South African legal system to respond to the risk and benefits posed by digitalisation. We argued that this question would be best answered by developing what we have termed a 'South African public law perspective'. In our view, while any particular legal system may often lag behind, the law constitutes an adaptive resource that can and should respond to disruptive technological change by re-examining existing concepts and creating new, more adequate conceptions. Our public law perspective reframes privacy law as *both* a private and a public good essential to the functioning of a constitutional democracy in the era of digitalisation.

We made two further arguments in our constitutional theory working paper. First, we found that the South African constitutional text instantiates a rights-orientated, and rule-of-law centred political theory, which potentially facilitates the development of a privacy law adequate for the Digital Age. In addition to the usual constitutional tools, South Africa's 'transformative constitution' has particularly apt characteristics for responding to digitalisation, including the component of horizontality (e.g. the application of constitutional norms to both public and private actors) and that of subsidiarity (e.g. meshing and calibrating legal frameworks at constitutional, legislative and judge-made levels).

We then discussed recent South African Constitutional Court cases addressing surveillance harms and other cases resolving disputes on harms associated with information's publication, dissemination, and use. Until recently, constitutional privacy jurisprudence in South Africa has not explicitly confronted the implications of impacts of disruptive technological change. Nonetheless, we argued that it has demonstrated the potential to do so. The opportunity exists to focus simultaneously on the need for systemic controls of harms to privacy and democracy and to recognise the need and benefits for digitalisation's impact sectors, such as law enforcement and social rights in this ultimately constitutional analysis.

In this working paper, we take the analysis one practical step further: we use our public law perspective on digitalisation in the South African health sector. We do so because this sector is significant in its own right – public health is necessary for a healthy society – and also to further

explore how and to what extent the South African constitutional framework provides resources at least roughly adequate for the challenges posed by the current 'digitalisation plus' era.[1]

The theoretical perspective we have developed is certainly relevant to digitalisation's impact in the health sector. The social, economic and political progress that took place in the 20th century was strongly correlated with technological change of the first three industrial revolutions.[2] The technological innovations associated with what many are terming 'the fourth industrial revolution' are also of undoubted utility in the form of new possibilities for enhanced productivity, business formation and wealth creation, as well as the enhanced efficacy of public action to address basic needs such as education and public health.[3]

As we explore more fully in Part Four below, digitalisation's potential for societal impact was on full display during the current COVID-19 pandemic. While many factors influenced social responses to the pandemic, and we do not suggest a direct relationship between digital infrastructure and effectiveness, we also note that some countries with advanced digital infrastructure, such as Korea, were able to respond relatively effectively in the early days of the pandemic. As an immunologist writing in the *Financial Times* observed recently: 'Efficient testing, tracing and containment was a soluble technological and organizational problem.'[4] The negative costs of 'technological lags' were also made plain in the case of South Africa. The government struggled to implement a technology-based contact tracing solution based on smartphone capability which impaired its response to the public health crisis.[5] Delays in the migration from analogue to digital broadcasting constrained the ability of our education authorities to expand online learning in disadvantaged communities under the lockdown regulations.

In this working paper, we focus only on the health sector. Our aim is to demonstrate our argument about the significance of a public law perspective on the constitutional right to privacy in the age of 'digitalisation plus' through raising and discussing several issues raised by digitalisation's impact in the particular sector of health. It would be possible and valuable to extend its analysis beyond health into any of numerous spheres of social life – from energy to education, and policing to

---

[1] Digitisation – the storing of information in digital as opposed to analogue or paper-based forms, e.g. storing information in computers as strings of zeros and ones – has had social and economic impacts since at least the 1960s. The pace and depth of these impacts has increased since around the middle of the first decade of this 21st century. Many speak now of a process of digitalisation as a social and economic process in its own right. Arjun Appadurai and Neta Alexander, *Failure* (Wiley 2019). We discuss the current moment – terming it the era of digitalisation plus – at pp. 3-4 of the accompanying paper.

[2] See Carl Benedict Frey, *The Technology Trap: Capital, Labor and Power in the Age of Automation* (2019). (Chapter 6 'From Mass Production to Mass Flourishing.')

[3] The potential social and economic benefits of digitalisation are also stressed by some writers on the political left. See for instance Roberto Unger, *The Knowledge Economy* (2019), who foresees the possibility of a knowledge economy for the many; and Eveny Mozorov 'Digital Socialism: The Calculation Debate in the Age of Big Data' *New Left Review* 116/117 March/ June 2019, discussing theories that postulate the possibility of Socialist economic planning as a result of information technologies and predictive analytics.

[4] Thiago Carvallo, *FT* 2nd –3rd January 2021. But some states also used the COVID-19 pandemic to increase their powers of surveillance over their citizens. China went so far as to install CCTV cameras inside people's homes or just outside their front doors, according to Veliz. See Carissa Veliz, *Privacy is Power: Why and How you Should Take Back Control Over Your Data* (2020) p.57.

[5] Jonathan Klaaren et al ' South Africa's Covid-19 Tracing Database: Risks and Rewards of which Doctors Should be aware', *South African Medical Journal*, June 2020 110(7).

child care. We mainly focus on technologies that have health benefits and privacy costs, but we also recognise that certain technologies have health costs and privacy benefits. Our main point is to demonstrate the value a constitutional right to privacy can bring to the regulation of digital technologies in a variety of legal frameworks and technological settings – from public to private, and from the law of the constitution to the 'law' of computer coding.

This working paper proceeds in three further substantive sections:

- Part Two recalls our public law perspective on digitalisation and the constitutional right to privacy and surveys the regulatory landscape of the health sector in South Africa. We briefly describe the operationalisation and application of health privacy regulation in post-apartheid society.

- This prepares us to, in Part Three, note and assess a number of specific digital health technologies currently in use in interventions in South Africa. To survey and assess instances of digitalisation's impact on health, we adopt the international World Health Organization (WHO) classification of digital health interventions. We thus are adopting a global conceptual structure to assist in our assessment of the current state of a national sector.

- In Part Four, we focus on the recent response to the COVID-19 pandemic and discuss the establishment in South Africa of the COVID-19 Tracing Database, and subsequent technological interventions aiming to enhance contact tracing and other responses. The initial database establishment was a development at the interface of the law enforcement and health sectors, which raised concerns regarding its risks to privacy, but also raised hopes regarding its potential rewards in protecting public health.

Part Two: The Health Sector in South Africa – a Regulatory Overview from a Public Law Perspective

As we have argued in *Digitalisation, the 'Fourth Industrial Revolution' and the Constitutional Law of Privacy in South Africa*, the working paper accompanying this one, the challenges that changes in digital technology pose to existing legal frameworks (including, but not limited to, privacy law) require the articulation of a public law perspective on the constitutional right to privacy. Accomplishing this task is likely to be enabled by South Africa's Constitution. This Constitution has two particularly relevant and developed doctrines – horizontality and subsidiarity – that are crucial for engaging with digitalisation and articulating an adequate framework of privacy law. Additionally, in 2013, South Africa authorised a regulator spanning the policy domains of privacy and access to information. And, in mid-2021, data protection provisions of South Africa's Protection of Personal Information Act (POPIA) come into effect. A further crucial set of legal resources (separate to POPIA) consist of the common law's capacity to continue to deal with many of the harms associated with digitalisation, and the potential of the constitutional right of privacy to specifically address collective harms, in addition to comprehensively overseeing privacy law.

The components of horizontality and subsidiarity are particularly relevant to the health sector in the age of digitalisation. For instance, the potential power wielded by electronic platforms is a good context for the horizontal application of rights, such as the right to health and the right to privacy. Therefore, there is a question specific to the South African context (and relevant for the constitutional theory engaged with in our accompanying paper): should horizontality – a concept and debate that has receded to some degree from doctrinal discussions over constitutional rights in South Africa from its earlier prominence in the early 1990s, when the Constitution and the Bill of Rights was being drafted – come back into our current discussion over privacy (and health) in South Africa as a useful and progressive concept? As for subsidiarity, its conceptual structure mirrors the comprehensive and powerful logic of digital technology, building its very coherence and structure as a network out of numerous individual links – for example, from constitution to legislation, from legislation to subordinate legislation, from subordinate legislation to regulatory interpretation, from regulatory interpretation to judge-made decisions and the like. Both components are, we argue, crucial for enabling law to respond to the costs and benefits of digitalisation.

South Africa's health sector has seen considerable change in the past 25 years. It has moved significantly in the direction of becoming a deracialised, comprehensive and integrated health system. As the government has recently noted, '[a]verage life expectancy at birth declined over the first decade of democracy, largely due to the devastating impact of the HIV and AIDS epidemic, reaching a low of 54 years in 2005. Since then, however, it has improved steadily, reaching 64.6 years in 2019.'[6]

[6] DPME, Towards a 25 Year Review: 1994-2019, Department of Planning, Monitoring and Evaluation, 2019 https://www.gov.za/sites/default/files/gcis_document/201911/towards25yearreview.pdf, accessed 7 September 2020.

One significant and celebrated feature of South Africa's health system is its relatively high rates of use of healthcare services. For instance, in 2015, 94% of pregnant women received antenatal care, 96% delivered in a healthcare facility, and 97% were attended at delivery by a skilled medical practitioner.[7] In absolute number terms, the use of public healthcare has increased dramatically, to some extent addressing an apartheid-era healthcare deficit. The number of such healthcare visits per annum has increased from 67 million in 1998 to 'close to 120 million annually by March 2019' with 71.5% of households using public sector clinics in 2018.'[8] Persistent challenges that remain include addressing the inequalities of cost and level of care between the public and the private healthcare sectors, the explosion of litigation and claims related to medical negligence against the state in recent years, and declining levels of community participation in healthcare provision.[9]

In addition to the professional and statutory bodies overseeing the work of the professionals and other personnel key to health sector, several other statutory bodies exist to regulate various non-personnel aspects of activity within the health sector. These include the South African Health Products Regulatory Authority (SAHPRA) and the Office of Health Standards Compliance (OHSC). SAHPRA has statutory authority to regulate clinical trials, medicines, and health devices. OHSC monitors health establishments' compliance with health standards. Significant activities, such as the establishment, licensing and funding of hospitals, remain regulated by officials at the national and provincial line departments of health, which share constitutional jurisdiction over this competence and implement the National Health Act 61 of 2003 and other sector legislation.[10] Other regulatory bodies set up by their own empowering statutes include the Compensation Commissioner for Occupational Diseases and the Road Accident Fund.[11]

To understand the privacy-related issues raised by the intervention of digital technology within the health sector (as discussed further in Part Three) we need to understand the regulation of health devices.[12] The regulation of these devices is within the competence of SAHPRA, a body built from the Medicines Control Council.[13] As currently implemented, SAHPRA's regulatory model has several key components, including the regulation of establishments and regulation through reliance:

- SAHPRA currently licenses establishments, though it does not require them to prove that their quality management systems are up to international standards.

---

[7] Yogan Pillay and Pakishe Aaron Motsoaledi, 'Digital Health in South Africa: Innovating to Improve Health' (2018) *BMJ Global Health* e000722.

[8] DPME (n 146) p.101.

[9] Ibid. p.103–104.

[10] Sasha Stevenson (ed), *National Health Act Guide* 2019 (3rd edn, SiberInk 2019) http://section27.org.za/wp-content/uploads/2019/07/Stevenson-National-Health-Act-Guide-2019-1.pdf, accessed 28 May 2021.

[11] Pieter Carstens and Debbie Pearmain, 'The Regulatory Framework of the South African Health System Comparative Health Systems Reform' (2009) *Medicine and Law 91*, 94.

[12] Catherine Tomlinson, 'The Tangled Web of Medical Device Regulation in SA' (*Spotlight*, 3 September 2020), https://www.dailymaverick.co.za/article/2020-09-03-the-tangled-web-of-medical-device-regulation-in-sa, accessed 4 September 2020.

[13] Jonathan Klaaren, 'Regulatory Politics in South Africa 25 Years After Apartheid' [2020] *Journal of Asian and African Studies*, 10 February 2021.

• SAHPRA also regulates the devices that such establishments (as well as ones outside South Africa's borders) produce through the key mechanism of reliance – meaning that, especially for high-risk products, if evidence is presented that the relevant devices are registered in one of six recognised jurisdictions, the device is eligible to meet the standards of section 21 authorisation and thus be marketed in South Africa. Reliance here refers to '"relying" on registration or authorisation in other countries.'[14]

An alternative route to these six jurisdictions is for a device to be pre-qualified by WHO. The six jurisdictions are: Australia, Brazil, Canada, the EU, Japan, and the USA. This reliance component to health sector regulation is similar to the reliance component of ICT regulation by South Africa's telecommunications and broadcasting regulator, the Independent Communications Authority of South Africa (ICASA). SAHPRA has demonstrated some capacity to respond to the COVID-19 pandemic with some agile regulatory arrangements, although it does not appear to be well co-ordinated with other important government entities, including the National Treasury and the National Department of Health (NDOH).[15]

International health regulations approved by the World Health Assembly, part of an international treaty system linked to WHO, generally become part of South African law via the International Health Regulations Act 28 of 1974. This international law was used by the WHO Director-General to declare the COVID-19 pandemic a public health emergency of international concern and to co-ordinate a global response.

It should be noted that we have not examined in any detail the regulatory instruments and processes by which it is possible that some (or even many) risks to privacy may be actively mitigated. Such processes may include the use of privacy and data protection impact assessments as employed in comparative jurisdictions.[16] For instance, s 19(2) of POPI requires a risk assessment that might be interpreted (or supplemented, as was the case with the Stellenbosch University Privacy Regulation) to include a privacy impact assessment.[17]

---

[14] Tomlinson (n 152).

[15] Ibid.

[16] Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) Vol. 25 Computer Law & Security Review 123; David Wright and Charles Raab, 'Privacy Principles, Risks and Harms' (2014) Vol. 28 *International Review of Law, Computers & Technology*, 277.

[17] Ciara Staunton et al., 'Protection of Personal Information Act 2013 and Data Protection for Health Research in South Africa' [2020] *International Data Privacy Law* ipz024.

Part Three: Digital Health Interventions in South Africa

The impact of digital technology globally has been considerable, and its impact on the health sector in South Africa has been no exception. Since around 2000, the term 'digital health' has been used to recognise and evaluate this development.[18] While it is not necessary to fully dive into the related literature here, one helpful line of analysis in gaining insight into the challenges and opportunities posed in this sector has been developed by WHO as an aid for policymakers. In 2018, WHO classified the full range of different digital health interventions as a tool towards understanding the impact of digital technology in health.[19]

Therefore, here we use the classification scheme of digital health interventions proposed by WHO to identify some of the current constitutional issues in the South African health sector occasioned by digitalisation. WHO's overview of digital technologies helpfully distinguishes four types based on the targeted primary user: health clients; healthcare providers; health system or resource managers; and data services. In this part of the report, we identify and briefly discuss a significant digital health intervention in each of these four primary WHO categories.

Health clients

Interventions directed at health clients include targeted client communication, personal health tracking, and on-demand information services. While there are many examples that could (and should) be examined further in this category,[20] we identify here just one: a client-focused technology developed in a public/private partnership: MomConnect.

The laudable and celebrated high rate of use of health services by pregnant women in South Africa is associated with a significant digital health intervention – MomConnect, technology developed by the NDOH and a range of implementers including the Praekelt Foundation, a private non-profit corporation.[21] The MomConnect service provides twice-weekly health information messages

[18] Simon C Mathews et al., 'Digital Health: A Path to Validation' (2019) 2 npj *Digital Medicine* 1.

[19] WHO, 'Classification of Digital Health Interventions v1.0: A Shared Language to Describe the Uses of Digital Technology for Health' (WHO 2018) https://apps.who.int/iris/bitstream/handle/10665/260480/WHO-RHR-18.06-eng.pdf, accessed 4 September 2020.

[20] For instance, as Adam B Cohen et al. observed: '[t]hese technological offerings can address unmet healthcare needs by circumventing traditional intermediaries, such as payers (eg, insurance companies and governments), clinicians, employers, and the pharmaceutical industry, and provide patients with direct access to health-related data and services. Like other industries that empower consumers with easily accessible information and services, direct-to-consumer digital health might similarly transform healthcare. Fitness trackers, sleep monitors, and wearables that detect arrhythmias are the current leading technologies. Direct-to-consumer healthcare already represents a US$700 billion industry and includes over-the-counter drugs, care management in retail clinics, hearing aids, glasses, contact lenses, and nutraceuticals.' 'Direct-to-Consumer Digital Health', *The Lancet Digital Health* 2, no. 4 (April 2020): e163–65, https://doi.org/10.1016/S2589-7500(20)30057-1, accessed 24 May 2021.

[21] Razzano, Gabriella. *Digital Hegemonies for COVID-19,* 5 November, 2020. http://globaldatajustice.org/covid-19/digital-hegemonies-south-africa, accessed 23 June 2021.

to pregnant women and allows them to submit compliments and complaints about the health services they have received at local level. MomConnect is argued to be innovative, in particular in incorporating registration of the pregnancies and in using interoperable technology.[22] Looked at with a global lens, MomConnect is one of only five mobile health information messaging programmes to have scaled to over one million beneficiaries. Further, it is the only programme across the world to have attained population-level coverage of more than 60%. There are privacy issues with this programme. It 'collects the user's identification number and facility code during registration, enabling future linkages with other health and population databases and geolocated feedback.'[23] As Barron et al. noted: '[t]he privacy, data security and confidentiality aspects of holding individual patient information in a national system in South Africa … came to the fore for the first time in MomConnect'. Rules and operating procedures were established for hosting and accessing such data, which are held on secure NDOH-controlled servers and subject to the same rules as other routine data systems.[24] Above and beyond these issues of informational privacy, the digital technology encompassed in MomConnect represents a significant use of private power, albeit for a public purpose. From a public law perspective, the regulation of this power is largely embedded in agreements and contractual framework rather than a framework of primary or subordinate legislation.

Healthcare providers

Digital health interventions directed at healthcare providers include client health records, referral co-ordination, and prescription and medication management. One challenge evident through the healthcare sector in South Africa is that of patient and healthcare worker autonomy and potential infringements on individual privacy. While using technology to facilitate the quality and delivery of healthcare, digital technologies may of course infringe on rights to privacy, intruding in particular into the liberal zones of individual privacy. Informational privacy issues may be associated with healthcare workers, as well as with patients and research participants. In respect of personal health records stemming from healthcare services, the advent of digital health has raised particular issues.[25] One issue is the access of patients to their own medical records in situations where a third party had an interest in those records. At least in part in response to changing business models enabled by digital technology, '[h]ealthcare practitioners are increasingly called upon to step out of their usual clinical role to evaluate and report on claimants for non-clinical purposes, such as eligibility for insured benefits.'[26] For the most part, the challenges posed by this second set of

[22] Ibid. p.1.

[23] Peter Barron et al., 'Mobile Health Messaging Service and Helpdesk for South African Mothers (MomConnect): History, Successes and Challenges' (2018) 3 *BMJ Global Health* e000559.

[24] Ibid. p.4.

[25] Floyd Els and Liezel Cilliers, 'A Privacy Management Framework for Personal Electronic Health Records' (2018) 10 *African Journal of Science, Technology, Innovation and Development* 725; Barron et al. (n 163). p.4.

[26] M van Niekerk, 'Providing Claimants with Access to Information: A Comparative Analysis of the POPIA, PAIA and HPCSA Guidelines' (2019) 12 *South African Journal of Bioethics and Law* 32.

technologies may be addressed through a combination of statutory and regulatory instruments. Going forward, the key statute will be POPIA and its interaction with the regulatory framework of the National Health Act. While the constitutional right to privacy will play a background and supervisory role, it is unlikely to need to provide the primary role in this category.

Health system or resource managers

Digital health technologies directed at health system or resource managers include technologies for supply chain management, public health event notification, civil registration and vital statistics, and health financing. At least one continued type of operation of South Africa's second-generation pandemic response technologies fits within this category as a public health event notification to health system managers – the use of data at the aggregate level for population mobility and COVID-19 hotspot mapping. As the successive technologies to the COVID-19 Tracing Database (discussed further in Part Four) have been developed and deployed, there has remained a residual thread of operations continuing at (among others) the Council for Scientific and Industrial Research (CSIR), the public organisation initially chosen to house the database, and which is in touch with a range of key public health entities, including the NDOH. Since May 2020, one of the major South African telecommunications companies, Vodacom, has provided aggregate data for use in population mobility estimates to several public entities including the CSIR, the National Institute for Communicable Diseases (NICD), the City of Cape Town, and the Free State and Eastern Cape provincial Departments of Health.

These estimates do not include individual contact tracing data. In a separate operation, the CSIR uses anonymised contact tracing data from the NICD to compile approximated COVID-19 hotspot maps.[27] This piece of hotspot mapping – which was also an ambition of the tracing database – from the point of view of the group right to reasonable inferences from data. In a related policy debate, some have asked whether the practice of disclosing specific infection statistics implicates the group right of privacy.[28] In many ways, the regulation of these technologies may primarily be a matter of the constitutional right to health and its interaction with the general limitations clause, section 36.

The purpose of most of the digital technologies in this third classification is to advance public health through the effective and efficient use of limited resources. However, the implementation of this effort is done through the full variety of statutory, regulatory, and private law-based instruments, as well as instruments not usually thought of as classically regulatory, such as information technology standards and computing languages and coding protocol. This welter of texts (and

[27] Jonathan Klaaren and Brian Ray, *South Africa's Technologies Enhancing Contact Tracing for COVID-19: A Comparative and Human Rights Assessment* (2021). https://doi.org/10.13140/RG.2.2.22982.40009, accessed 23 June 2021.

[28] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI Survey: Privacy, Data, and Business' (2019). *Columbia Business Law Review* 494.

codes) is reflective of the fast-changing health sector in the 21st century. As can be inferred from the parallel surveillance context of the AmaBhungane case,[29] the constitutional right to privacy may well find employment here via either or both of the horizontality and the subsidiarity doctrines noted above.

Data services

Digital health technologies directed towards data services include data collection, management and use, data coding, locational mapping, and data exchange and interoperability. One practice in this category that poses issues at the interface of technology and privacy is biorepository (or biobank) research in Africa. Biorepository research is based on the collection, processing, storage, and distribution of biological materials for future health research. Spreading globally and growing rapidly since around 1990, in part due to the facilitation and acceleration of digital technology, several biorepositories have been established in Africa in the last 20 years, associated with the development of bioinformatics and computational biology. Treading in sensitive terrain from the point of view of decoloniality as well as privacy, the pending application of South Africa's privacy law to its biorepository research facilities raises important questions of lawfulness as well as the continuing ability of South African facilities to collaborate with their African counterparts in jurisdictions without robust privacy laws and enforcement.[30] There are between 10 and 20 iorepositories in South Africa that currently fall under the somewhat ambiguous regulation of the NDOH and the National Health Laboratory Service.[31]

The now-inoperative COVID-19 Tracing Database – with its avowed purpose of using geolocational data for contact tracing – also falls squarely within this final WHO category and is discussed further in the Part Four. The regulation of this set of technologies includes cross-border agreements with both public and private entities and falls at the intersection of the constitutional rights of privacy, health, and academic freedom (the right to research).

Unsurprisingly, technological developments along the above lines have resulted in several recent disputes in the South African courts. One pitted two South African health and life insurers against each other in the High Court, debating whether the publicly available scoring system of one could be used commercially by the other.[32] Another dispute has seen an enquiry (launched in July 2019)

[29] Please see accompanying paper at pp.22-25, discussing AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others (CCT 278/19; CCT 279/19) [2021] ZACC 3 (4 February 2021).

[30] Staunton et al. (n 157); DW Thaldar and B Townsend, 'Genomic Research and Privacy: A response to Staunton et al.' (2020) 110 *South African Medical Journal* 172; C Staunton et al., 'Safeguarding the Future of Genomic Research in South Africa: Broad Consent and the Protection of Personal Information Act No. 4 of 2013' (2019) 109 *South African Medical Journal* 468.

[31] Pamela Andanda and Sandra Govender, 'Regulation of Biobanks in South Africa' (2015) 43 *The Journal of Law, Medicine & Ethics* 787.

[32] Discovery Ltd and Others v Liberty Group Ltd (21362/2019) [2020] ZAGPJHC 67; [2020] 2 All SA 819 (GJ); 2020 (4) SA 160 (GJ) (15 April 2020).

by several well-respected senior advocates into the question of whether medical schemes' data analysis practices have unlawfully discriminated against claims lodged by African and Indian medical practitioners, resulting in an interim report and threats of court actions.[33] Both of these cases fall within the category of data services.

Informed by the doctrines of horizontality and subsidiarity, a privacy law developed by the public law perspective we have detailed in our accompanying paper can provide a powerful and flexible instrument for engaging with the issues posed by the digital technologies of all these types. A fundamentally reconceptualised privacy right cannot on its own address the regulatory issues identified in the health sector. But it can engage with private power, such as that on display in several instances above, perhaps most notably in the technologies directed at data services. And it is able to interact with the multiple obstacles and opportunities posed at multiple levels: by other constitutional rights, by statutes including, but not limited to, POPIA and the National Health Act, by subordinate legislation, by professional standards, agreements and other instruments using private law to accomplish public ends, and even by some avenues of control not usually thought of as within the purview of a Constitution at all, such as standards and computing codes.

[33] Khomotso Mabelane, 'Report into Medical Aid Schemes' Racial Profiling yet to Be Released', *POWER 98.7*, 10 August 2020, https://www.power987.co.za/news/report-into-medical-aid-schemes-racial-profiling-yet-to-be-released, accessed 3 September 2020.

Part Four: The COVID-19 Tracing Database and subsequent technological initiatives to enhance digital contact tracing in South Africa

In addition to the more gradual change caused by the onset of digital technology in the health sector, the sudden onset and extensive duration of the COVID-19 pandemic has sparked sharp change, much of this also taking place through digital technology. One prominent example in the health sector was the series of attempts by the South African Government to enhance and empower state contact tracing capacity. These efforts have raised a number of privacy issues, similar to those identified and discussed in Part Three. The first of these attempts – the COVID-19 Tracing Database – lies in the overlap between the health sector and law enforcement.

While these developments are covered in depth elsewhere,[34] a brief overview of this series of technological interventions helps to identify potential risks and rewards, and to understand how these are assessed within the current regulatory privacy regime. It also demonstrates the key argument of our public law perspective on constitutional privacy law in the era of digitalisation – that South Africa's constitutional regime possesses the fundamental legal resources, although not the decided body of case law, to engage with the full spectrum of benefits (social and economic) as well as harms (surveillance and dissemination) that are emerging in contemporary South African and global society.

In response to the COVID-19 pandemic, South Africa engaged in a sequence of attempted technological enhancements to the crucial pandemic-fighting function of contact tracing. Each of these attempts presents a case of pushing the integration of digital technology into existing systems (or the creation of a new system) to achieve public health. In the first of these efforts, the government established a tracing database in March and April 2020. This technology aimed to collect both aggregated and individualised mobility and geolocational data on COVID-19 cases and their contacts. With its broad and deep evidence base, the database had the potential to assist health system managers with policy formulation and to provide a database to assist with contact tracing, thus falling into the third and fourth of WHO's classifications. Arguing that there were both risks and rewards, we have published reports on the establishment of this database soon after its establishment, effectively cautiously noting its possibility to assist with public health.[35]

About four months into South Africa's pandemic response, the NDOH announced that the tracing database was no longer operating, although the legal machinery for the database and its oversight remain in place. As things happened, while there were no judicial responses to the privacy risks of the tracing database, it turned out that a privacy-guaranteeing regulatory structure – the appointment of a designed judge with a mandate to oversee privacy protection and make recommendations to government – was instrumental in noting and communicating the inability

[34] Klaaren and Ray. (n 27).

[35] J Klaaren et al., 'South Africa's COVID-19 Tracing Database: Risks and Rewards of Which Doctors Should be Aware' (2020) 110 *South African Medical Journal*, http://www.samj.org.za/index.php/samj/article/view/12983, accessed 4 June 2020.

of the tracing database to perform its function due to the lack of precision in the key category of data it had decided to collect – geolocational data. In layman's terms, the triangulated information gathered from cellphone towers simply was not clean or precise enough to assist materially with contact tracing.[36] This is an example of a 'technological lag', one arguably negatively impacting South Africa's response to the pandemic.

South Africa's replacement initiative within this space was COVIDConnect, a technology developed by Telkom/BCX and the Praekelt Foundation partnering with the NDOH.[37] According to BCX, the COVIDConnect app '[a]llows the public to screen for COVID-19 on WhatsApp …; [s]hares test results and provides advice to those who have tested positive for COVID-19 through GovChat's LetsTalk line …. [a]n SMS is sent to inform when results are available; [and a]nonymously alerts people who may have been in close contact with someone who tests positive for COVID-19.'

Further, COVIDConnect 'draws data from various data sources and provides district health teams with the ability to search for individuals via a table interface, giving them direct communication with the individual via SMS [through building] a map view of SA with functionality to filter by province and include all primary infected individuals listed on the system, whilst identifying the close contacts and [h]eat map overlays indicate the volumes of infected relative to population estimates.'

COVIDConnect differs from applications used elsewhere by relying on persons testing positive with COVID-19 to voluntarily provide the names and contact details of their contacts.[38] Its power to engage in hotspot mapping – which was also an ambition of the tracing database – is within the ambit of one part of the developing concept of privacy discussed above, the right to reasonable inferences from data. With its dual focus on clients as well as healthcare managers, this second technological intervention straddles the first and the third of WHO's categories discussed in Part Three (health clients; and health system or resource managers).[39]

In its third major technological intervention, on 1 September, the government launched COVID Alert SA, a Bluetooth application and part of the Google/Apple Exposure Notification (GAEN) system operated by Google and Apple. This was stated to be part of the COVIDConnect platform.[40] With its strong privacy protections and its limited aims, this technology fits squarely back within WHO's first category – digital health interventions directed at health clients. South Africa's ambitions to technologically support contact tracing – at least judging by the high-profile technological interventions surveyed here – have been directed to clients and health system managers and

[36] Klaaren and Ray (n 27). (Text at notes 11-13)

[37] 'BCX and the Department of Health Partner to Launch COVIDConnect' (BCX, 22 July 2020), https://www.bcx.co.za/insights/bcx-and-the-department-of-health-partner-to-launch-covidconnect, accessed 2 September 2020.

[38] Elri Voigt, 'The Trial and Error of Covid-19 Digital Contact Tracing in South Africa', *Maverick Citizen*, 28 July 2020, https://www.dailymaverick.co.za/article/2020-07-28-the-trial-and-error-of-covid-19-digital-contact-tracing-in-south-africa, accessed 31 July 2020.

[39] Klaaren and Ray (n 27). (Text at notes 49-57)

[40] National Department of Health, South Africa, 'Download the App - Every COVID Alert SA App Download Means More Lives Saved in SA', COVID-19 Online Resource & News Portal, 1 September 2020, https://sacoronavirus.co.za/2020/09/01/download-the-app-every-covid-alert-sa-app-download-means-more-lives-saved-in-sa, accessed 2 September 2020.

not to healthcare providers, nor to the data systems providers. Furthermore, their development appears to be more significantly influenced by the capacity of the state to work with the private sector to devise such initiatives as well as the availability of the technologies, rather than by any clearly defined campaign to counter new threats to privacy or popular backlash along such lines.[41]

[41] Klaaren and Ray (n 27). (Text at notes 69-72)

Part Five: Conclusion

We have briefly surveyed the regulatory structures in the South African health sector and some of the interventions made by digital technologies impacting in that sector. We have drawn from both the South African public law perspective on the constitutional law of privacy in the era of digitalisation and from a global regulatory classification of digital health technologies. We have also presented an account of the series of technological attempts the South African Government embarked on to enhance and empower state contact tracing capacity early in the COVID-19 pandemic.

There are several policy implications that flow from this research, two of which we note here:

Perhaps the most important echoes a point made in our accompanying paper (one flowing from the doctrine of horizontality) – the need to acknowledge the public and private nature of the social action at issue in these questions. This need is shown in our account of the South African technological responses to the COVID-19 pandemic as well as in the overview of the numerous technological interventions in the health sector. Policymakers who examine either the public or the private sides of these social questions and their potential answers are unlikely to enable an adequate and effective response.

We also call for policymakers to acknowledge and monitor the costs and the benefits these technologies are causing our society to incur. Policy instruments such as privacy impact assessments should be considered as important tools. Such assessments can be used to guide social and economic regulatory choices before the event, and to document and chart the complexity of the impacts of the technologies afterwards.


BLAVATNIK
SCHOOL OF
GOVERNMENT
UNIVERSITY OF
OXFORD


Digital
Pathways
at Oxford