Digitalisation, the 'Fourth Industrial Revolution' and the Constitutional Law of Privacy in South Africa: Towards a public law perspective on constitutional privacy in the era of digitalisation

Digital Pathways Paper Series
DOI: https://doi.org/10.35489/BSG-DP-WP_2021/04

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 14
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). *Digitalisation, the 'Fourth Industrial Revolution' and the Constitutional Law of Privacy in South Africa: Towards a public law perspective on constitutional privacy in the era of digitalisation*. Digital Pathways at Oxford Paper Series; no. 14. 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

…that which was intended to enlighten the world in practice darkens it.
James Bridle

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

He lives well who is well hidden.
Descartes

Table of Contents

Part One: Introduction

The Information Society and digitalisation

The 'Information Society' – the roots of which can be traced back to efforts after the Second World War to improve the predictability of weather patterns by combining the information gathering and retrieval abilities of new computing equipment and modern systems of electronic communications to analyse vast amounts of data – is at an inflection point.[1] To take just one representative and significant instance, consider the views of Klaus Schwab, Founder and Executive Chairman of the World Economic Forum. Schwab has characterised this phase of 'Digitalisation' – involving a much more ubiquitous and mobile internet, smaller more powerful and cheaper sensors, artificial intelligence and machine learning – as a ' fourth industrial revolution', distinguishing this current phase of rapid and disruptive technological change from earlier iterations.[2'3] According to Schwab, the combination of information technology, artificial intelligence and biotechnology heralds the possibility of the integration of the physical and virtual worlds and of the biological body and machines in a 'post human' world. This raises some fundamental questions about the way we understand ourselves and the way we organise our societies, economies and polities. The most basic commitments of constitutional democracy to individual agency and collective self-determination may now be under threat by disruptive technological change.[4]

Schwab's 'digitalisation as progress' story, which we will examine more closely below, accurately presents digitalisation as a global process. But this global process has impacts within states and is perhaps primarily responded to at the national level. While the context for our analysis is global, our specific focus is on the response of the South African legal system to technological change. South Africa underwent its transition from apartheid to constitutional democracy 25 years ago, thus only truly (and democratically) joining the international community comparatively recently. It faces many socio-economic challenges arising from this legacy and its subordinate positioning in the global economy. And it must also face up to many contemporary 'wicked problems'[5] including those associated with the 'fourth industrial revolution' *as a constitutional democracy.*

---

1 James Bridle, *New Dark Age: Technology and the End of the Future* (Verso Books 2019) p.25.

2 Klaus Schwab, *The Fourth Industrial Revolution* (Penguin UK 2017) p.7.

3 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).

4 Schwab (n 2) p.46.

5 S Woolman, *Wrecking Ball: Why Permanent Technological Unemployment, A predictable Pandemic and Other Wicked Problems Will end South Africa's Experiment In Inclusive Democracy* (2021). 'Wicked problems' are a distinct class of collective action problems that are difficult to resolve and may prove intractable if only because they require action over the long term by multiple actors at state and global level in the absence of adequate global institutions.

Case law, data protection, and the right to privacy

In this working paper, our focus is on the constitutional debates and case law regarding the right to privacy, adopting a method that is largely theoretical. In an accompanying separate working paper, *A South African Public Law Perspective on Digitalisation in the Health Sector*, we employ the analysis developed here and focus on the specific case of digital technologies in the health sector.

The topic and task of these papers lie at the confluence of many areas of contemporary society. To demonstrate and apply the argument of this paper, it would be possible and valuable to extend its analysis into any of numerous spheres of social life, from energy to education to policing to child care. In our accompanying separate paper, we focus on only one policy domain – 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, and attend to several issues raised by digitalisation's impact in the health sector. For the most part, we focus on technologies that have health benefits and privacy costs, but we also recognise that certain technologies have health costs and privacy benefits. We also briefly outline the recent establishment (and subsequent events) in South Africa of a contact tracing database responding to the COVID-19 pandemic – the COVID-19 Tracing Database – a development at the interface of the law enforcement and health sectors. Our main point in this accompanying paper is to demonstrate the value that 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.

Before turning to the detail of South Africa's legal and constitutional response to digitalisation below, it is worth further examining the differences between at least two perspectives on digitalisation which are in a constructive tension with each other.

The premise of Schwab's book, as we pointed out above is basically optimistic.[6] Technology and digitalisation, he says 'will change everything' and have 'great benefits' although Schwab does not entirely overlook some 'big challenges ' such as deepening systemic inequality since 'the great beneficiaries of the fourth industrial revolution are the providers of intellectual or physical capital – the innovators, the investors, and the shareholders.'[7] He also concedes that data protection laws are currently inadequate in many jurisdictions, but maintains that 'the rules around the collection, processing, and reselling of personal data are now well defined in Europe.'[8] User profiling through 'big data analysis and inference techniques' Schwab says 'is opening the way for new more customized and personalized services that can benefit users and consumers.'[9]

[6] See his most recent book, (Klaus Schwab and Peter Vanham, *Stakeholder Capitalism: A Global Economy that Works for Progress, People and Planet* (2021)) in which, while retaining this basic posture, he confronts the harms associated with digitalisation, which include growing income inequality and the market power of Platform companies.

[7] Schwab (n 2) pp.10–12.

[8] This is a contentious matter in many non-OECD jurisdictions. African countries, like those in Asia, are increasingly enacting data privacy laws that adhere closely to European models. Still, there remain 18 of 55 national jurisdictions in Africa without data protection laws or legislation in the pipeline. Further, no African country obtained a positive assessment of the 'adequacy' of their data protection system from the European Union under the 1995 Data Protection Directive, although the EU did carry out some unilateral assessments. Graham Greenleaf and Bertil Cottier, *Comparing African Data Privacy Laws: International, African and Regional Commitments*, April 22, 2020, https://papers.ssrn.com/abstract=3582478, accessed 28 May 2021.

[9] Ibid. p.8.

The era of digitalisation plus

Evaluations such as Schwab's – which we see forming part of a view of 'digitalisation as progress' – are deeply rooted in the cultural and intellectual history of industrialising societies, which in the 'West' is associated with the 'Enlightenment' and the birth of modernity. Consider Steven Pinker's observation in *Enlightenment Now: The Case For Reason Science, Humanism, And Progress*, '[t]echnology doesn't just improve old things; it invents new ones.'[10] Pinker's assessment of the possibilities that come with the new phase of digitalisation, which we style 'digitalization plus'[11] also has a positive directionality: 'The innovations in the pipeline are not just a list of cool ideas. They fall out of the overarching historical development that has been called the New Renaissance and the Second Machine Age.' This new phase of technological history has a 'revolutionary promise' – that information technology can guide and exponentially improve all other technologies, extending beyond computer power to technologies such as genomics. The process of innovation itself is undergoing a significant series of innovations. As Pinker points out, one of these innovations is: 'the democratization of platforms for invention … the economic empowerment of billions of people through smartphones, online education and microfinancing.'[12]

The social, economic and political progress that took place in the 20th century is indeed strongly correlated with technological change of the first three industrial revolutions.[13] The technological innovations associated with 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 public health and education.[14]

The latter is in evidence during the current COVID-19 pandemic. While many factors influenced responses (of public institutions) to the pandemic, (and we do not suggest a direct relationship between digital infrastructure and efficacy), we also note that some countries with advanced digital infrastructures, 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,

[10] Steven Pinker, *Enlightenment Now: The Case for Reason, Science, Humanism, and Progress* (Penguin UK 2018) p.82.

[11] By 'digitalization plus' we are referencing the transition already under way from the 'Information economy' to the 'data economy' and from the 'Third Industrial Revolution' to the 'Fourth Industrial Revolution' that is characterized by quantum computing and a fusion of technologies which blur the lines between the physical, digital and biological spheres. See Klause Schwab and Peter Vanham, *Stakeholder Capitalism: A Global Economy that works for Progress, People and Planet* (2021) at pages 137-145

[12] Ibid. pp.331–332.

[13] 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')

[14] 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 which postulate the possibility of Socialist economic planning as a result of information technologies and predictive analytics.

tracing and containment was a soluble technological and organizational problem.'[15] 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.[16] Delays in the migration from analogue to digital broadcasting constrained the ability of our education authorities to expand online learning in disadvantaged communities under lockdown regulations.

The fourth industrial revolution

Concern that Africa and South Africa are 'falling behind as a result of the exponential growth in technology'[17] and that we will not be able to share in the benefits of the fourth industrial revolution led South Africa's President to establish a Fourth Industrial Revolution (4IR) Commission recently. This commission has proposed that we should: invest in human capital; establish a platform for advanced manufacturing; secure and avail data to enable innovations; incentivise future industries; build 4IR infrastructure; and establish an artificial intelligence (AI) institute and a 4IR Strategy Implementation Council in the Presidency.[18] The Independent Communications Authority of South Africa (ICASA), the country's telecommunications regulator, is now prioritising the auctioning of infrastructure to facilitate the incorporation of next-generation 5G technology mobile telephony[19] after a delay of implementation for a decade. These developments show that the South African State seeks to be become a more active force, facilitating technological change to foster economic development and improve the efficacy of public action.[20] Its policy discourse is now increasingly dominated by a mainly positive evaluation of the economic and other public benefits of next-generation digitalisation and is determined to 'catch up'.

Another critical view emerging in universities and civil society on the turn to digital presents an alternative to this 'sunny perspective' (shared by Corporate South Africa). This second view, which we share, sees 'digitalisation as progress' as being informed by an uncritical teleology that underestimates the potential costs of 'digitalisation plus'. In our view, these costs (which include, but are not limited to, privacy costs – the specific focus of this paper) must also be considered in fashioning a long-term regulatory and policy response to technological change. Facets of

[15] Thiago Carvallo, *FT* 2-3 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 See Carissa Veliz, *Privacy is Power: Why and How you Should Take Back Control Over Your Data* (2020) p.57.

[16] 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).

[17] Tshilidzi Marwala, *Closing the Gap: The Fourth Industrial Revolution In Africa* (2020) p.1.

[18] Ibid. p.26.

[19] *Legal Brief elaw Issue no.1866.* This is being opposed by TELKOM, the country's third largest mobile operator and former state monopoly.

[20] Many other states agree – for instance, the Chinese State is committed to ' innovation led Growth' and building China into a Cyberpower. See Xi Jinping: *The Governance of China* (2018).

what we term 'digitalisation plus' call into question the simple association of digitalisation with linear 'progress': Edward Snowden's revelations about secret mass surveillance by the National Security Agency in the USA; public disclosure that social networking platform Facebook had sold the data of its users to Cambridge Analytica, which enabled it to shape voter preferences and influence the outcome of elections; growing awareness of how technology platform companies like Google (supposedly just a 'search engine') track our online lives to attract advertising revenue and monetise personal data; and the corrosive impact on public deliberation and the democratic process of the dissemination of false information.[21]

South Africa: surveillance state?

The critical perspective argues that South Africa is in danger of either becoming a surveillance state or has indeed already partially become one.[22] As was confirmed in the *AmaBhungane* case, there is evidence that South Africa has established its own mass surveillance centre, as well as having manufactured, exported and imported mass surveillance technologies.[23] Calling on the South African Government to publicly disclose the surveillance technologies capacities of the law enforcement security service and to regulate the export of surveillance technologies by private companies based in South Africa, the civil society body, The Right2Know Campaign, made submissions to the UN Human Rights Committee for the ending of mass surveillance in October 2016.[24] The Committee found South Africa's compliance with its international obligations inadequate to protect the right to privacy observing:

> 'The Committee is concerned about the relatively low threshold for conducting surveillance … and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the Regulation of the Interception of Communications Act and Provision of Communications Related Information Act 70 of 2002. … The Committee is further concerned at reports of unlawful surveillance practices, including mass interception of communications carried out by the National Communications Centre and the delays in operationalizing the Protection of Personal information Act, 2003, due in particular to the delays in the establishment of an Information Regulator…'[25]

[21] See Julian Baggani, *A Short History of Truth: Consolations For a Post-Truth World* (2017).

[22] Keith Breckenridge, 'The Biometric State: The Promise and Peril of Digital Government in the New South Africa', *Journal of Southern African Studies* 31, no. 2 (June 1, 2005): pp.267–82, https://doi.org/10.1080/03057070500109458, accessed 28 May 2021; Jane Duncan, *Stopping the Spies*, 1st ed. (Wits University Press, 2018).

[23] Duncan, p.117; *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).

[24] Ibid. p.17.

[25] *Human Rights Committee Concluding Observations on the Initial Report on South Africa*, CCPR/ZAF/1, 27 April (paras 42-43).

The Committee concluded that South Africa 'should take all necessary measures to ensure that its surveillance activities conform to its obligations under the ICCPR, including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality.'[26] In 2018, Professor of Journalism, Jane Duncan published her book *Stopping the Spies: Constructing and resisting the surveillance state in South Africa*, in which she assesses the relevance of Snowden's revelations for South Africa, and asks whether South Africa is becoming a surveillance state.[27] In her view, '[e]lements of a surveillance state are manifesting themselves most strongly in relation to the intelligence services, although there are signs that the police have been increasing their intelligence-gathering activities and have at the very least been attempting to develop their own capabilities.'[28]

Privacy and social media platforms

Among South African civil society actors, there are also growing concerns about the deleterious impact on the constitutional right to privacy and on the quality of public deliberation of misinformation posted or 'published' on social media platforms like Facebook and Twitter. South Africans have had their own 'Cambridge Analytica' case in the exposure of British consultancy Bell Pottinger's role in deepening racial tensions in South Africa through a social media campaign.[29] The Oxford Internet Institute, which tracks public opinion online, has recently added South Africa to the growing list of countries where social media is being used to peddle misinformation and computational propaganda.[30] According to Anton Harber, former editor of the *Mail & Guardian* and now a professor in the Wits School of Journalism, 'Social media is enabling the spread of misinformation on a scale and speed never seen before, and often this disinformation is intended to spread hate, violence and conflict… We are now seeing how in the US and UK such misinformation has contributed to a poisonous political atmosphere and the decline of their democracy.'[31]

[26] *The Right to Privacy in South Africa: Stakeholder Report: Universal Periodic Review 27th Session - South Africa 16th October 2016* submitted by the Right2Know Campaign.

[27] Jane Duncan, *Stopping the Spies* (1st edition, Wits University Press 2018).

[28] Duncan, p. 221.

[29] David Segal, 'How Bell Pottinger, P.R. Firm for Despots and Rogues, Met Its End in South Africa' www.nytimes.com/2018/02/04/business/bell-pottinger-guptas-zuma-south-africa.html (cited in Victoria Bronstein and Judith Katzew, 'Safeguarding the South African Public Broadcaster: Governance, Civil Society and the SABC', *Journal of Media Law* 10, no. 2 (3 July, 2018): 244–72, https://doi.org/10.1080/17577632.2018.1592284, accessed 28 May 2021.

[30] Legal Brief e law. Issue no.1866 (citing 2020 edition of the Oxford Internet Institute's Global Inventory of Organized Social Media Manipulation).

[31] *Business Day*, 20 October 2021.

Public law perspective on the right to constitutional privacy

It is with attention to both the largely positive discourse on digitalisation's potential impact on South African society as well as our caution about its costs that we embark in this paper on the development and illustration of our public law perspective on constitutional privacy. Our research question is to ask what legal resources (such as the doctrines and concepts of 'constitutional rights', 'proportionality', 'horizontality' and 'subsidiarity' as well as others) which are embodied in various legal instruments ('Judge-made' law, statute law, regulations, and the constitutional text) and are implemented by various institutions (the legislature, courts, regulatory bodies, etc.) are available in the South African legal system post 1994 (i.e. as a 'constitutional democracy') to respond/adapt to the risks and benefits of digitalisation?

We explore this question from what we call a 'South African public law perspective'. The development of this perspective has been enabled by the adoption of a constitution, a 'transformative constitution' with particular characteristics. These include the component of horizontality, under which constitutional norms apply to both public and private actors. Before 1994, privacy in South Africa was solely a 'private law'/common law/delictual matter. Effectively, the regulation of privacy was the composite of actions (court cases under the common law) for damages between sets of private parties. Apart from anything else (the lack of democracy and denial of human rights) South Africa's pre-1994 legal system had severe limits as a vehicle for responding to technological change.

Our perspective on the right to constitutional privacy in South Africa foregrounds questions of legal ordering which necessarily engage the normative foundations of constitutional democracies. 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 on its citizens? How can that information be appropriately shared with persons and firms in the private sector 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?

This perspective does not ignore the benefits of digitalisation, but is sceptical of the claims of the autonomous functioning of digital technologies and of their inevitably benign transformative purposes. Hence the need for constitutional control. We focus attention on how the design of new-generation technologies is being shaped by the interests and imperatives of states and private corporations and on systemic harms to privacy and the functioning of constitutional democracies. As Jathan Sadowski has recently observed: 'By uncovering the technopolitics of smart tech, we … see how their impacts go far beyond the usual set of concerns about privacy intrusions and cybersecurity breaches.' Corporate and governmental power is amplified by these 'sophisticated tools' in Sadowski's view. 'They are transformative technologies that are being used to shape society in profound ways'[32] not all of them benign. [33]

[32] Jathan Sadowski, *Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over The World* (2020), p.12.

[33] Ibid. p.17.

We therefore postulate the need for the development of a public law perspective on privacy, and particularly of one grounded in constitutional norms. Such a perspective must:

(a) start with an examination of the 'internal logic' and capabilities of digital technologies to identify the harms to which privacy law must now be responsive[34]

(b) situate this reconsideration of privacy law in the context of the harms, risks and power dynamics[35] generated by digitalisation and the way these technologies are being used by governments and the private sector[36]

(c) examine the 'balances' to be struck between 'the costs and benefits' of digitalisation in a constitutional democracy with its particular set of commitments to both individual self-determination and collective self-determination, and to the Rule of Law.

The structure of this report

We have divided our working paper into several parts. **Part Two** develops and articulates a theoretical perspective which informs our 'public law perspective on constitutional privacy in the era of digitalisation' by discussing privacy law, contextually in relation to state power, the logics of surveillance capitalism, and the functioning of constitutional democracies.

Turning more explicitly to legal frameworks, **Part Three** considers the constitutional right to privacy in the context of South Africa's transformative constitutionalism and its potential to respond to the harms of digitalisation. Part Three argues that the South African Constitution instantiates a rights-orientated and rule of law centred political theory which potentially facilitates the development of a privacy law for the Digital Age. This privacy law includes but goes beyond the regulatory domain of data protection. Here, we lay out two important but unremarkable ways in which the text of the South African Constitution augments the conceptual resources available for judicial reasoning in the field of South African law of privacy. Part Three then covers some quite distinctive features – subsidiarity and horizontality – which enhance the role of constitutional law in responding to technological change in our jurisdiction.

After surveying transformative constitutionalism, private power and constitutional privacy, **Part Four** engages in a discussion of the Constitutional Court's case law on the right of constitutional privacy, dividing that discussion into the recent Constitutional Court cases addressing surveillance harms and those resolving disputes addressing the harms associated with publication, dissemination, and use. We then finish the paper in **Part Five** with a short conclusion.

[34] Op. cit. Carissa Veliz. p.27.

[35] Op. cit. Sadowski. pp.38-42.

[36] Lawrence Lessig, *Code: 2.0* (2006) p. xv.

Part Two: Towards a public law perspective on constitutional privacy in the era of digitalisation

The discussion in this part considers: (a) privacy law; (b) the state and capital; and (c) the interaction of democratic self-government and privacy.

(a) Digitalisation 2.0: Privacy law

Law is an adaptive resource that can and should respond to disruptive technological change by re-examining existing concepts and creating new, more adequate conceptions. This was the basic 'problematic' of the famous and foundational article by Warren and Brandeis[37] in which they proposed that privacy should be recognised as a specific delictual right in the light of the harms to individuals created by new technologies like hand-held cameras.[38] In their articulation of this right, it was a 'right to be left alone'.[39]

As we have detailed, digital technology today is more than a step beyond hand-held cameras. Today privacy law should direct attention to the amplification of the privacy harms arising from 'datafication' and 'smartification' associated with mobile computing, cloud computing, the Internet of Things, and machine learning, data mining and predictive analytics. Balkin has observed: 'As we move from the world of the internet to Algorithmic Society, the horizons of our concerns must expand.'[40] Daniel Solove's article, although published some time ago, provides a useful starting point for assessing these enhanced risks and harms. There are four basic groups of potentially harmful activities under his taxonomy:

1) information collection
2) information processing
3) information dissemination
4) invasion.[41]

Each of these groups consists of different related groups of potentially harmful activities. Solove's taxonomy can, for the most part, accommodate an analysis of the risks to privacy in the current period of accelerated digitalisation, but with some modifications. The amplified risk associated with digitalised 'Big Data' of intentional and negligent data spills resulting from the failure of public and private record-keepers to secure their databases, for example, can be understood with reference to the risks inherent in the collection, aggregation and processing of increasing

[37] Samuel D. Warren and Louis Brandeis 'The Right To Privacy' *Harvard Law Review*, vol.4,No.5. (Dec. 15,1890), pp.193-220.

[38] Ibid. p. 195.

[39] Ibid. p. 195.

[40] Jack Balkin, 'Information Fiduciaries and The First Amendment', *University of California Davis* Vol. 49:1183, 1234.

[41] Daniel. J. Solove ' A Taxonomy of Privacy' *University Of Pennsylvania Law Review* Vol. 154, No 3. January, 2006 477, p.488.

volumes of information across data sets by numerous public and private organisations.[42] He also anticipates the harms associated with decision-making concerning the 'digital person' based on pooled data from many data sources. But he does not specifically discuss the harms related to data mining and predictive analytics increasingly relied upon by public organisations to allocate public benefits and by private commercial organisations to monitor the preferences and behaviours of their 'customers.'[43] In this regard, Sandra Wachter and Brent Mittelstadt have recently argued that the EU General Data Protection Regulation (GDPR), which was adopted on 25 May 2018, grants individuals little control over how their personal data is used to draw inferences that might damage their privacy and reputation, and that there is therefore a need for recognition for a new data protection right to 'reasonable inferences.'[44] As Carissa Veliz points out 'institutions for knowing more about us can escape the limits set for them through inferring, rather than collecting, sensitive information about us.'[45]

Soloves's taxonomy also usefully recognises the architectural or structural impact of state surveillance enabled by the new digital technologies on power dynamics between states and individuals.[46] But his focus is on the harms to the individual that result from the digitalised recording of information. This misses the systemic and collective nature of privacy harms that is now becoming evident. As Veliz pointed out recently: 'Privacy is not only about you... Privacy is as collective as it is personal…privacy resembles ecological issues and other collective action problems.'[47] That your data is personal seems to imply that you are the only concerned party when it comes to sharing it. Veliz shows that this is not necessarily the case.[48] The sharing of genetic information, for instance, can impact on others in a family group, though we may not be aware of this when we decide to share this information.

These 'externalities' and 'information asymmetries' have important implications for how we think about the harms and risks that privacy law has to be responsive to today. It calls into question the framing of privacy as an exclusively individual and private right designed to remedy discreet, direct and immediate harms to individuals. Both the common law and statutory data processing law (focusing largely on notice and consent) are based on this conceptual edifice. However, this individualistic framing of the privacy right is no longer fully adequate when 'we ourselves are utterly enmeshed in technological systems, which shape in turn how we act and how we think. We cannot stand outside them. We cannot think without them.'[49] Data protection itself may implicate other rights beyond privacy such as equality and dignity.

---

[42] Omri Ben-Shahar 'Data Pollution' *Journal of Legal Analysis* Vol 11 (2019) p.105. Omri challenges the view that the injuries from 'digitalisation 2.0' are exclusively private. He argues instead that personal information that is shared in the digital economy undermines and degrades public goods and interests, and therefore that legal framings which assume harms exclusively to individual interests like privacy and tort law are inadequate.

[43] Baroso. p.355.

[44] Sandra Wachter and Brent Mittlestadt 'A Right to Reasonable Inferences: Rethinking Data Protection Law in The Age Of Big Data and AI' 2019 *Columbia Business Law Review.* 494 (2019).

[45] Op. cit. Veliz, p.134.

[46] Op. cit. Veliz, p.499.

[47] Op. cit. Veliz, p.75.

[48] Ibid. p.76.

[49] Op. cit. Bridle, p.2.

The addition of a group of activities potentially harming our social and collective existence through their systemic impact – akin to Solove's current item of 'invasion' but without that item's individualistic conceptualisation – would be a valuable modification to his typology of potentially harmful groups of activities. In the following sections, we present arguments to support the idea that privacy should be reframed from a public law perspective as *both* a private and a public good essential to the functioning of a constitutional democracy.

(b) Digitalisation 2.0: The state and capital

Solove's 2006 analysis of the privacy harms that arise from the information practices of public authorities also gives insufficient attention to the way digitalisation augments the state's powers of surveillance and the contemporary accretions of private power associated with platform companies like Facebook, Amazon and Google. It has become increasingly clear that the analysis of the privacy harms associated with digitalisation must be situated within the context of the political economy of 'Surveillance Capitalism'[50] or 'Digital Capitalism.'[51]

The modern bureaucratic state apparatus has always had to systematically 'map' its subjects and citizens by gathering and recording information in order to carry out its public functions.[52] And even those with a restrictive role of the state's economic and social functions accepted the Hobbesian[53] view that the state had to provide security and that its policing powers had to include powers of 'search and seizure.'[54] Digitalisation exponentially expands the powers of the contemporary state's bureaucratic powers of computation, control[55] and surveillance, leading some scholars to turn to Foucaultian concepts such as 'biopower ' and 'disciplinary power' to examine the way digitalisation is fundamentally restructuring power relations between individuals and the state: 'The symbol of disciplinary power is the panopticon....The symbol of control is the computer network that invisibly, constantly and continuously records every action... control systems do not rely on mere threats of surveillance. They follow through on monitoring, judging and inhibiting your freedom…'[56]

Law enforcement agencies in many countries are also increasingly relying on 'Big Data' to investigate crime and on 'dragnet' surveillance technologies like CCTV cameras, GPS locational technologies and drones purchased from companies manufacturing the high-tech tools for 'smart policing'.[57] Such 'dragnet' technologies operate at a wholescale or systemic level, rather than through individualised thresholds. These capabilities are of undoubted value in combatting

[50] Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019).

[51] Op. cit. Sadowski.

[52] Rob Lucas 'The Surveillance Business' *NLR* 121, Jan-Feb 132

[53] Ibid. pp.140-141.

[54] The Fourth Amendment of the US Constitution.

[55] Gilles Deleuze, 'Postcript on Societies of Control' *L'Autre Journal*, no.1 (May 1990).

[56] Op. cit. Sadowski p.41; Veliz Chapter 3.

[57] Op. cit. Sadowski. Chapter 7.

sophisticated organised crime and transnational crimes such as money laundering. But pervasive, systemic surveillance comes at a substantial cost to privacy and the freedoms that are essential to our ability to function and flourish in a community.

The extent to which the South African Police Service is relying on these technologies is not publicly known because of inadequate oversight mechanisms and constraints on parliamentary reporting.[58] Also, under South African law, law enforcement agencies are not required to observe the statutory processing rights of data subjects and so are not constrained by principles of data minimisation when investigating actual crimes or even suspected criminal conduct.[59] Digitalised surveillance and crime investigation techniques based on data analytics obviously raise some important questions about the adequacy of 'search and seizure'[60] privacy law premised on a conception of a spatial boundary between public and private space, which is now obsolete.

To properly situate the threats to privacy – to the functioning of constitutional democracies in the digital age – it is necessary to focus on these accretions of state power but also on the 'logic of accumulation' in the 'Age of Surveillance Capitalism'[61] as ownership of the 'means of behavioral modification eclipses ownership of the means of production as the fountainhead of capitalist wealth and power in the 21st century.'[62] Consciously invoking Marx, Zuboff shows how an extractive economic logic has developed on the infrastructural backbone of 'smart computing' which instrumentalises the most human and personal experiences to the commercial ends of platform companies and turns personal data into capital.[63] These network companies have morphed into behemoth monopolies whose competitive advantage is increasingly tied to their control of the 'new oil' of personal data which is sold to other businesses as a commercial asset. Protection of privacy rights is therefore now also a competition law issue.[64] Where required to do so, information collected and aggregated on the infrastructural backbone of these platform companies is also passed on to the surveillance state, creating a symbiotic relationship between the state and capital. In these circumstances a conceptualisation of privacy as a private harm threatened only by 'state action' is an obstacle to the development of a privacy law for the digital age.[65] The harms associated with private commercial power must also be reckoned with.

---

[58] Report submitted by Right2Know Campaign and Privacy International to the 27th Session of the UN Human Rights Commitee on the Right to Privacy in South Africa, October 2016, paras 41-45.

[59] The Protection of Personal Information Act 4 of 2013 (POPIA). Section 6(1)(c) (i) and (ii) exclude the processing of personal information by or on behalf of a public body for purposes of public safety as well as for the purposes of investigation and prosecution of crime.

[60] The 4th Amendment of the US Constitution has been reinterpreted to include non-physical searches. In *Olmstead vs the United States 277 US438 (1928)* the Supreme Court held that wire tapping by the police was not a 'trespass' and therefore not an invasion of privacy. Justice Brandeis dissented. The court reversed itself in *Katz vs the United States 389 US 347(1967).*

[61] Op. cit. Zuboff.

[62] Ibid. p.12.

[63] Op. cit. Sadowski. p.40.

[64] A court in Berlin (6th Division) has ruled in administrative proceedings that Facebook's privacy settings violate consumer and data protection laws. This was a decision under section 32 of the German Competition Act.

[65] Laurence Tribe, *The Constitution in Cyberspace: Law and Liberty beyond the Electronic Frontier*. Tribe defends the limited reach of the US Constitution in the form of the 'state action doctrine'.

(c) Democratic self-government and privacy

Accretions of public and private power, and surveillance and monopolistic power, associated with 'Digital Capitalism' have some important implications for the functioning of democracies as a system of democratic self-government which requires us to think about the relationship between privacy and democracy. The harms to democracy arise from the processing capabilities of digital technologies, which have facilitated the dissemination of polarising propaganda and false information. Reliable procedures for arriving at agreement on the facts by public deliberation are essential to the functioning of democratic societies which aim at structuring conversation among a variety of opinions and interests. The capabilities enabled by digitalisation have also weakened the mass media and political parties. They also represent a real danger to the integrity of elections since the evidence is now clear that voter preferences can be manipulated through more targeted advertising and psychological profiling.[66] The accretions of private power associated with digitalisation and their intersection with public power are also accentuating underlying tendencies towards plutocracy and oligarchy in constitutional democracies today.[67] This undermines the claims of their systems of authority to be based on popular consent and political equality.

Therefore, the capabilities enabled by digital technologies and the power dynamics that have been unleashed require a reinvigoration of commitment to individual self-determination as well as to democratic self-government and a recognition of their interdependence. Under a public law paradigm, privacy today is much more than a negative individual right[68] not to be interfered with by the state. It is also required as a defence against private power and a positive right essential to the functioning of a constitutional democracy based on the rule of law. In the digital era and the pervasive system of surveillance, we need a richer concept of the constitutional value of 'privacy' in constitutional democracies than the right merely 'to be left alone.' Privacy must be understood as being integrally related to individual autonomy and agency.[69] In *Bernstein v Bester* the first privacy case in South Africa in the post-apartheid era, Justice Ackermann pointed in this direction in introducing a 'communitarian' reading of the value of constitutional privacy. He said:

> 'the scope of privacy has been closely related to the concept of identity and it has been stated that "rights like the right to privacy are not based on the notion of the unencumbered self, but on the notion of what is necessary to have one's own autonomous identity."'[70]

Understood in this way, privacy is not only a right to withdraw from society, but to be able to participate on respectful terms in a community of equals and without the constant external pressure of being watched, profiled and assessed by the state and commercial entities.[71]

---

[66] Op. cit. Veliz. p.102.

[67] Firoz Cachalia, 'Precautionary Constitutionalism, Representative Democracy and Political Corruption' (2019) 9 *Constitutional Court Review* 45.

[68] Isaiah Berlin, *Two Concepts of Liberty*, Oxford University Press (1969)

[69] Op. cit. Veliz. p.72.

[70] *Bernstein and Others v Bester NO and Others (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996)* [65].

[71] Op. cit. Veliz. p.72.

Part Three: Transformative constitutionalism and the constitutional right to privacy

Prior to the adoption of a new South African Constitution in 1996[72] as part of South Africa's transition to democracy, privacy was a purely private law matter regulated by the common law[73] that granted a course of action between individuals for the publication of defamatory statements and private facts.[74] In layman's terms, the primary legal recourse for defamation was going to court and proving one's case in front of a judge. Judge-made law within this paradigm had some potential to evolve incrementally[75] in response to changing facts, including those of technological change. But its conceptual structures and immanent logic are no longer entirely fit for purpose when considered in the light of contemporary harms to privacy, which are also (as we have pointed out) systemic and collective. We ask: what textual and interpretive resources are there under the post-1996 Constitution to develop a public law perspective on privacy law which is more responsive to the harms associated with 'digitalisation plus'? Our argument is that the South African constitutional text instantiates a rights-orientated, and rule of law centred political theory which potentially facilitates the development of a constitutional law of privacy more adequate for the Digital Age.

(a) Judicial review, constitutional rights and the principle of proportionality

There are two important but unremarkable ways in which the text of the South African Constitution augments the conceptual resources available for judicial reasoning in the field of South African law of privacy. The first is that it entrenches (as do many modern constitutions and human rights instruments)[76] a constitutional right to privacy. Section 14 of the Bill of Rights (chapter 2 of the Constitution) provides as follows:

'Everyone has the right to privacy, which includes the right not to have:

a) their person or home searched
b) their property searched
c) their possessions seized; or
d) the privacy of their communications infringed.'

[72] *Constitution of the Republic of South Africa* no.108 of 1996.

[73] The *actio iniuriarum*.

[74] For an overview of this case law, see Jonathan Burchell, 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid', *Electronic Journal of Comparative Law* 13, no. 1 (March 2009): 1–26 (updating Brandeis and Warren, but arguing that a tort or delictual action remains the best way to safeguard privacy in a combined common law and constitutional law context).

[75] O' Keeffe, recognising a right to privacy under the *actio iniuriarum*.

[76] Article 17 of the International Covenant of Civil and Political Rights; and article 13 of the European Convention. The African Charter of Peoples and Human and People's Rights does not expressly protect privacy rights.

It is important to note that the post-apartheid introduction of the Bill of Rights including a constitutional right to privacy by no means extinguished the common law, which continues as part of the South African legal system, albeit controlled by the Constitution as the supreme law. Furthermore, as we note below, the South African Parliament's 2013 privacy legislation created a statutory right to privacy (which comes fully into effect in mid-2021) and a regulator for privacy rights, and for the constitutional right of access to information.

Second, various other provisions of the Constitution read together create a strong system of judicial review. Section 7(1) provides that the Bill of Rights 'is the cornerstone of democracy' which in terms of section 7(2) the state is required to 'respect, protect, promote and fulfil'. The Bill of Rights applies to all law and conduct,[77] and binds the legislature, the executive and the judiciary.[78] Section 167 concentrates the power to decide questions of constitutionality in the Constitutional Court. This includes parliamentary legislation[79] and 'all law' which must comply with the rights provisions of the Bill of Rights and the founding value of the rule of law.[80] The Constitution can therefore be understood as setting up a system of constitutional dialogue between the judiciary and the elected branches which enhances the capacity of the legal system to respond to disruptive technological change.

The constitutional text thus creates rich normative and interpretive resources for the Judiciary to attribute meaning to the constitutional right to privacy as the centrepiece of privacy law in light of the harms associated with digitalisation. The Bill of Rights of the South African Constitution also includes other fundamental rights, such as the right to equality[81] and to dignity,[82] which can support the development of a 'public law perspective'. In a case concerning an action for defamation against a media company under the common law, Justice Kate O'Regan said the following about the symbiotic relationship between the constitutional right to privacy and another constitutional right, the right to dignity:[83]

> 'The value of human dignity in our constitution therefore values both the personal sense of self-worth as well as the public's estimation of the worth or value of an individual. It should also be noted that there is a close link between human dignity and privacy in our constitutional order. The right to privacy, entrenched in section 124 of the constitution, recognizes human beings have a right to a sphere of intimacy and autonomy that should be protected from invasion. This right serves to foster human dignity. No sharp lines then can be drawn between reputation, dignitas and privacy in giving effect to human dignity in our constitution.'[84]

---

77 Section 2 (contained in Chapter 2, the Founding Provisions).

78 Section 8.

79 Section 167(b).

80 Op. cit. Modderklip. Section 2.

81 Section 9.

82 Section 10.

83 *Khumalo and Others v Holomisa (CCT53/01) [2002] ZACC 12; 2002 (5) SA 401; 2002 (8) BCLR 771 (14 June 2002)* [27].

84 Ibid. p.27.

The core constitutional value of dignity in this reasoning works in two ways. First, it reinforces privacy as a liberty which protects intimacy and individual choice from interference mainly by the state or third parties. Second, the constitutional value of dignity also recognises and protects an individual's interest in public estimations of an individual's worth. This distinct conception of dignity and privacy has greater potential to reach the harms associated with digitalisation since these harms can much less plausibly be conceptualised as intrusions in protected spaces or individual decisions. They relate to the right to control information about oneself that may be published or disseminated on digital platforms. Some jurisdictions, including South Africa, have therefore given recognition to a specific right to informational privacy.[85]

Constitutional rights to privacy and dignity in the South African Constitution are 'strong' rights which cannot be simply be weighed against some supposed public benefit.[86] They can only be limited in accordance with principles of proportionality expressly set out in section 36 of the Constitution itself. The limitation clause provides as follows:

'The rights in the Bill of Rights may be limited only in terms of a law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking in to account all relevant factors, including:

a) the nature of the right;
b) the importance and purpose of the limitation;
c) the relation between the limitation and the purpose; and
d) less restrictive means to achieve the purpose.'

Section 36 embeds the limitations analysis in the normative framework of a constitutional democracy. It therefore enables the court to undertake a broader harm analysis (which can include systemic harms) when assessing the constitutional adequacy of legal rules of general application, and to carefully examine both the ends and means of the legislature's legislative decisions in light of the constitutional commitment to privacy and dignity. Mere utilitarian balancing of costs and benefits is obviously excluded.

[85] James Q. Whitman ' Two Western Cultures of Privacy: Dignity vs Liberty' *Yale Law Journal* Vol.13, 2004 1153. See in particular his discussion of the protection of personality rights under German privacy law and the importance attached to the value of dignity.

[86] Strong rights as we understand them in the South African context are rights that can only be lawfully limited by satisfying the requirements of proportionality. Utilitarian balancing is not sufficient. Such rights according to Tushnet are ones well institutionalised in a particular society and may also achieve that strength through weak forms of judicial review with non-judicial actors also enforcing them. Mark Tushnet, *Weak Courts, Strong Rights: Judicial Review and Social Welfare Rights in Comparative Constitutional Law* (Princeton University Press, 2009).

(b) Constitutional supremacy, subsidiarity and horizontality

The South African Constitution also has some quite distinctive features – in particular, the doctrines of subsidiarity and horizontality – which further enhance the potential for constitutional law to respond to technological change in our jurisdiction. In its continued development of these doctrines in the 'digitalisation plus' age, the Constitutional Court will have to stay abreast of rapidly changing technologies and shoulder much of the responsibility.

The doctrine of subsidiarity is the founding principle of constitutional supremacy[87] read with its correlate, the judge-made rule of subsidiarity. Parliamentary legislation (as indicated above) is required to comply with constitutional norms in order to be valid. The legal norms created by legislation are therefore subsidiary ones in our legal system. Where the wording of a constitutional right requires that the legislature 'give effect' to the constitutional right,[88] litigants are usually required to proceed in the first instance on the basis of the more concrete statutory right and not directly on the basis of the constitutional right.[89] But the Constitutional Court has effectively embellished the statutory right with a constitutional gloss by insisting that statutory right has to be interpreted in light of the norms of the more abstract constitutional right.[90] So the constitutional right provides the governing norm, even after the legislature has enacted legislation giving effect to a constitutional right.

In other places, the Constitution does not expressly require a legislative enactment, as is the case with the constitutional right to privacy (at least if that right is assumed to be sourced entirely in section 14). In any case, giving at least partial effect to the constitutional right to privacy, Parliament has recently enacted a privacy law in the form of data protection legislation, the Protection of Personal Information Act 4 of 2013 (POPIA).[91] Among other things, this law establishes an Information

[87] Section 1 provides that the Republic of South Africa is one sovereign, democratic state founded on the following values: c) Supremacy of the Constitution and the Rule of Law.

[88] As does, for instance, the right to lawful, reasonable and procedurally fair administrative action in section 33. Jonathan Klaaren, 'Constitutional Authority to Enforce the Rights of Administrative Justice and Access to Information' (1997) 13 *South African Journal on Human Rights* 549.

[89] *My Vote Counts NPC v Speaker of the National Assembly and Others (CCT121/14) [2015] ZACC 31 (30 September 2015); My Vote Counts NPC v Minister of Justice and Correctional Services and Another (CCT249/17) [2018] ZACC 17; 2018 (8) BCLR 893 (CC); 2018 (5) SA 380 (CC) (21 June 2018);* Raisa Cachalia, 'Botching Procedure, Avoiding Substance: A critique of the majority judgment in My Vote Counts' (2017) 33 *South African Journal on Human Rights* 138; Jonathan Klaaren, 'My Vote Counts and the Transparency of Political Party Funding in South Africa' (2018) *22 Law, Democracy, & Development* 1; Melanie Murcott and Werner van der Westhuizen, 'The Ebb and Flow of the Application of the Principle of Subsidiarity - Critical Reflections on Motau and My Vote Counts Administrative Law' (2015) 7 *Constitutional Court Review* 43.

[90] *Grey's Marine Hout Bay v Minister of Public Works 2005(6)SA 313(SCA).*

[91] The Constitutional Court has assumed that a right to information privacy exists in terms of section 13, the constitutional right to privacy. *Mistry v Interim National Medical and Dental Council and Others* (CCT13/97) [1998] ZACC 10; 1998 (4) SA 1127; 1998 (7) BCLR 880 (29 May 1998) paras 47-48 (deciding case on the assumption that the constitutional right to privacy includes information privacy). It thus remains arguable that an alternative or supplemental text for a right of informational privacy is the constitutional right of access to information. When drafting the legislation enforcing the right of access to information, Parliament deferred the question of data protection legislation to the South African Law Reform Commission. Jonathan Klaaren, 'The Right of Access to Information at Age Ten', in *Reflections on Democracy and Human Rights: A Decade of the South African Constitution* (South African Human Rights Commission, 2006), pp.167–71.

Regulator charged with enforcement of both the rights of access to information (section 32) and of privacy (section 14) and arranges for the transition of regulatory responsibilities from the South African Human Rights Commission to the Information Regulator.[92]

A fascinating case in January 2021 from the Constitutional Court grappled with the doctrine of subsidiarity precisely at the interface between common law and a statute giving effect to a constitutional right, the right to equality. In *King*, the judiciary faced a complex fact pattern concerning the enforceability of several interconnected wills.[93] The question presented was whether to develop the common law or to depend on the Equality Act to counter the effects of gender discrimination while enforcing the freedom of testation. The common law provided at least as clear an option to counter gender discrimination than did one relevant part of the statutory framework. Seeing the issue through the indirect lens of the common law, the court minority would have developed the common law while the majority opinion instead opted not to do so, achieving the desired result via direct application of either the constitutional right of equality or the law giving effect to that right (the Equality Act). Most interestingly for our purposes here, one judge concurring with the majority wrote separately to argue for a more direct and robust application of the Equality Act, doing so on the basis of subsidiarity. Explaining her concurrence, Victor AJ wrote '[e]vidently, this case requires direct application as opposed to indirect application. The direct application of the Bill of Rights, however, must be consonant with the principle of constitutional subsidiarity. Therefore, in applying the Bill of Rights directly in this case, reliance must be placed on the Equality Act because its definition of unfair discrimination 'covers the field.'[94]

While we align our public law perspective with that of Victor AJ, there is one crucial difference between the equality question she addressed and the privacy-centred topic we treat here: the scope of the legislation enforcing the constitutional right or at least some part of it. In our view, Parliament's recently enacted privacy legislation does not cover the whole field of the constitutional right to privacy.[95] POPIA is an important statute with a significant role, but it does not even claim to exhaustively treat the full scope of questions of interest. While it is not the purpose of this paper to answer them, clearly questions with regard to the relationship between the constitutional right to privacy and the statutory rights and structures created by the Act will arise. Although the Act defines 'personal information' and 'processing' very broadly, it does not cover all the privacy harms associated with digitalisation, particularly surveillance and dissemination harms.[96] Section 14 of

[92] R Adams and F Adeleke, *Protecting Information Rights in South Africa: The Strategic Oversight Roles of the South African Human Rights Commission and the Information Regulator* http://repository.hsrc.ac.za/handle/20.500.11910/15085, accessed 18 February 2020.

[93] *King NO and Others v De Jager and Others (CCT 315/18) [2021] ZACC 4 (19 February 2021).*

[94] Ibid. p.190.

[95] The right to privacy does not cover all the constitutionally cognisable harms associated with digitalisation. Decision-making by algorithm will raise other rights challenges to decisions made by public and private bodies relying on digital technologies. Discriminatory decisions could, for instance, be challenged on equality grounds, and unfair or unreasonable ones, under the Right to administrative justice under section 33 of the Constitution.

[96] Section 6 excludes data processing for law enforcement purposes, but only to the extent that adequate safeguards for the protection of personal information has been established in other legislation. Such envisaged legislation has not yet been enacted. Section 7 excludes journalism.

the Constitution will therefore continue to occupy a central place, (if not *the* central place) in the development of our privacy jurisprudence in response to technological change.[97]

The Constitution also explicitly confers law-making powers on the Constitutional Court by empowering the court to develop the common law in light of the Constitution's normative commitments. Section 7(2) provides for the horizontal application of a right to bind a natural or a juristic person, depending on the nature of the right and any duty imposed by the right. The question of whether the constitutional right to privacy applies horizontally (against private actors) or only vertically (against public actors) will certainly arise. This is because privately owned companies are very much an integral part of the political economy of Surveillance Capitalism. Where a right applies horizontally, the courts are empowered by section 8(3) to:

> 'develop the common law to the extent that legislation does not give effect to that right, and may also develop the rules of the common law to limit the right in accordance with the limitation clause of the constitution. We have already seen that there is no legislation which covers the field of privacy harms in their entirety and can be said to give full 'effect' to the constitutional right. Further, section 39(2) provides that, when developing the common law every court must promote the spirit, purport and objects of the Bill of Rights.'

The cumulative effect of these provisions is that all privacy law in South Africa is effectively constitutional law. As the late Justice Chaskalson observed in *Pharmaceutical Manufacturers*: 'There is only one system of law. It is shaped by the constitution, which is the supreme law, and all law, including the common law, derives its force from the constitution and is subject to constitutional control.'[98] Therefore, the meaning attributed to the constitutional right to privacy by the judiciary and the effect of that right on other existing legal frameworks ranging from statute to subordinate legislation to agreements to common law doctrines will be the central question in the digital age in South African privacy jurisprudence. It is a question which, as we will see in the case analysis to follow, has received little attention until recently.[99]

---

[97] Anneliese Roos, 'Privacy in the Facebook Era: A South African Legal Perspective', *South African Law Journal* 129, no. 2 (January 1, 2012): 375–402 (arguing that South African privacy law, including the constitutional right to privacy, can adapt to the challenges posed by social networking services).

[98] *Pharmaceutical Manufacturers Association of South Africa and Another: In re Ex Parte President of the Republic of South Africa and Others (CCT31/99) [2000] ZACC 1; 2000 (2) SA 674; 2000 (3) BCLR 241 (25 February 2000)* [44].

[99] A debate over the content of an African conception of privacy has recently spilled into the pages of scholarly journals. This raises a question beyond the scope of this paper: whether there exist specifically African notions of privacy which might, for instance, require a different understanding of the balances to be struck between such an understanding of 'privacy' and the obligations and duties of the state in the area of public health. Makulilo, 'The Quest for Information Privacy in Africa' (2018) 8 *Journal of Information Policy*, 317.

(c) Transformative constitutionalism, private power and constitutional privacy

The text of the South African Constitution has certain unique provisions which distinguish our version of the constitutionalist ideal from the 'classical' version in the balance it strikes between 'conservation' and social change. Another particularity of the South African Constitution is the fact that it reaches both public and private power. This was Karl Klare's central point in his influential 1998 article in which he argued that the transformative potential of the recently enacted constitution could be unlocked if the Judiciary abandoned formalist interpretive practices and recognised the imperative to contribute to the realisation of the political project instantiated in the text by adopting a 'post liberal' theory of adjudication.[100] By 'transformative constitutionalism' Klare meant 'a long term project of judicial enactment, interpretation and enforcement committed … to transforming the country's political and social institutions and power relations in a democratic, participatory and egalitarian direction.[101] Klare then pointed to various textual provisions to provide the evidence for his case for transformative adjudication.

The main focus of the work of the generation of scholars who enthusiastically embraced Klare's work was not on expansive readings of equality[102] and socio-economic rights,[103] and not constitutional privacy. But the two sets of provisions that Klare drew attention to in making his case for transformative constitutionalism will certainly be relevant to the development of our law of privacy in the digital age: section 7(2) which the imposes affirmative duties on the state and sections 8(2); and (3) which extends the application of the Constitution's rights provisions, including potentially the constitutional right to privacy, to private relationships regulated by the common law and thus potentially directly to 'private power'.

Klare's characterisation of the South African Constitution as 'transformative' is broadly accepted in the legal community. Such scepticism as there has been has concerned the limits of constitutional law as an instrument of progressive social change[104] and whether transformative constitutionalism requires judicial interpretive practices informed by Critical Legal Theory. Theunis Roux[105] has argued that the progressive purposes of the Constitution (for which he agrees there is ample textual evidence) can just as easily be realised by conventional adjudicative practices informed by a 'Dworkinian'[106] conception of the political morality that should inform constitutional reasoning.

[100] Karl E Klare, 'Legal Culture and Transformative Constitutionalism' (1998) *South African Journal on Human Rights* 146, 151.

[101] Ibid. p.153.

[102] Cathi Albertyn ' Adjudicating Affirmative Action within a Normative Framework of Substantive Equality and the Employment Equity Act: An opportunity missed? South African Police Service v Solidarity Obo Barnard' *South African Law Journal*, vol.132 (part 4) 2015.

[103] S Wilson and J Dugard 'Taking Poverty Seriously: the South African Constitutional Court and Socio-economic Rights' *Stellenbosch Law Review* 2011, 3.

[104] S Sibanda 'Not Purpose Made! Transformative Constitutionalism, Post Independence Constitutionalism and the Struggle to Eradicate Poverty' (2011) *Stellenbosch Law Review* 482.

[105] T Roux 'Transformative Constitutionalism and the Best Interpretation of the Constitution: Distinction Without A Difference' (2005) 2 *Stellenbosch Law Review*, 258.

[106] See Ronald Dworkin's last book *Justice for Hedgehogs* (2011), particularly Part Two.

We agree with Roux to this extent: rights and rule of law constitutionalism provides rich resources for the development of privacy rights protections in the digital age. But we also think that, for the Constitutional Court to develop a harm principle in the field of privacy rights, judges might have to 'step outside the text' and the universe of legal norms to examine not only how technologies 'work' (the 'Brandeis paradigm'), but also the power relations associated with the surveillance state and digital capitalism. Klare's understanding of adjudication as inevitably 'political' lends itself more naturally than Dworkin to judicial interpretive practices which incorporate consideration of the implications of 'power relations' which we believe a 'public law perspective' on constitutional privacy must take account of. This raises questions about the boundaries of constitutional law as an interpretive practice. For example, can constitutional law function more like competition law,[107] a field of law in which it is necessary to analyse how digital markets actually work and which also examines a range of formal and informal legal frameworks?[108] Constitutional Court Judges will understandably be reluctant to stray into uncharted waters, which threatens to erode the distinction between 'law' and 'politics.' But an overanxious regard for existing boundaries will limit the ability of the court to respond to the harms to constitutional democracy associated with digitalisation.

[107] In the 'Digital Plus' age , competition law is also going to have to reckon with the intersection between market efficiency and consumer privacy. Our proposed Public Law perspective on constitutional privacy grounded in non utilitarian constitutional norms sets up an interesting tension between the 'privacy of the consumer' and 'privacy of the person' which will be for the Constitutional court to resolve exercising its Jurisdiction as the final arbiter of the meaning and scope of constitutional rights.

[108] The doctrine of subsidiarity opens up consideration of this approach – which could marry the rules-based regulation of constitutional law with a more common-law method, akin to that used by economists in complex competition cases assessing the particularities of market boundaries and competitive dynamics, in a regulatory framework drawing on statutes, other regulatory instruments, and decided lower court case law.

Part Four: The South African Constitutional Court's privacy jurisprudence

The right to constitutional privacy has been invoked in only a handful of cases in the democratic era. And until this year it has not had to engage explicitly with the implications of digitalisation for privacy rights. But this existing body of case law will probably frame its reasoning in future cases. Some departures and new formulations will be necessary if the court is to respond to the harms associated with 'digital surveillance' by the state and its law enforcement agencies, and harms that come from the increasing aggregation and dissemination of data by private companies and especially by platform companies for commercial purposes. We examine in this section two types of cases, the first concerning the state's coercive powers of 'search' and 'surveillance' and comprising four Constitutional Court cases, and a second concerning constitutional control of the publication of private facts under the common law, as yet made up of cases decided by lower courts.

(a) Search, seizure and surveillance

The first and leading Constitutional Court case in South African privacy law is *Bernstein vs Bester*, a 'search' case.[109] Justice Ackermann provided an extended exposition of the philosophical underpinnings of the right to privacy and comparative jurisprudence, much of it not necessary for coming to a decision in the case. Although decided under section 13 of the 'Interim constitution'[110] all subsequent cases have invoked the core elements of his reasoning, sometimes somewhat formulaically, and generally avoided any further reflections on the content and scope of constitutional privacy.

The case involved a challenge to the constitutionality of sections 417 and 418 of the Companies Act which provided for the directors, officers and persons known or suspected to be in possession of any property of a company in a 'winding up' to be summoned and to be required to answer questions. The attack was based on the section 13 right to personal privacy and the right not to be subject to the seizure of private possessions or the violation of private communications.[111]

The court, distinguishing place, relationship and person-oriented conceptions of privacy came to the conclusion on the facts that it could not be said that there had been an invasion of private living space, any specified relationship or that the information within the knowledge of a director, officer or auditor of a limited liability company regulated by law fell within such person's personal privacy. With regard to the determination of the scope of the right, Justice Ackermann's adopted

[109] *Bernstein and Others v Bester NO and Others (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996)* (n 62).

[110] Constitution of the Republic of South Africa 200 of 1993.

[111] *Bernstein and Others v Bester NO and Others (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996)* (n 62) para 55.

the 'reasonable expectations' test. Under this test there is an inviolable 'inner sanctum' such as family life, sexual preferences, and the home which becomes progressively more attenuated as individuals enter into public spaces and communal relationships with others.[112] The test has found an enduring place in the court's privacy jurisprudence and will be important in future cases concerning the impact of digitalisation on constitutional privacy.

The test is drawn from US Fourth Amendment law.[113] Under this test, a party seeking to establish an unconstitutional invasion of the right to privacy by the government must have 'a *subjective expectatio*n of privacy that the society has recognized as *objectively reasonable*'. Announcing this test of an unconstitutional search, the *Katz* case significantly reversed the US Supreme Court's earlier decision of *Olmstead*.[114] That case had held, over an eloquent dissent by justice Brandeis, that wiretapping did not amount to a 'trespass'. Since there was no physical entry, there was no unconstitutional 'search'. The formulation of the new test in *Katz* was an attempt at preserving an original conception of freedom that technological change had erased. The aspiration, says Lawrence Lessig 'was to draw a line around private spaces that reflected our … understanding of privacy, in the light of the current potential of technology…'[115]

But in the age of 'digital surveillance' these original understandings of the boundary between the private and public domains, and accordingly of the application of the *Katz* test are obsolete.[116] Digital technologies, as Lessig has observed elsewhere, '… change … radically. They not only make more behavior monitorable; they also make more behavior searchable. The same technologies that gather data now gather it in a way that makes it searchable. Thus increasingly life becomes a village composed of parallel processors, accessible at any time to reconstruct events or track behavior.'[117] Lessig thus asks, we believe appropriately, will we need a second kind of privacy: 'privacy in public'?[118]

The respected jurist, Justice Langa, appeared to open the door to a reconsideration of the application of the 'reasonable expectations' test in South Africa in the light of technological change in *Investigating Directorate, Serious Economic Offences v Hyundai Motor Distributors* decided some years after *Bernstein*.[119] This was not a case concerning the reliance of the prosecuting authorities on advanced monitoring and data-recording technologies in investigating crime. It concerned the constitutionality of legislation which did not specifically require that the prosecuting authorities show a reasonable suspicion as a condition precedent when applying for a judicial

[112] Ibid. p.67.

[113] *Katz v US* 389 US (1967) p.362.

[114] *Olmstead v US* (1928)

[115] Lawrence Lessing, *Fidelity and Constraint: How the Supreme Court Has Read the American Constitution*. Oxford University Press, 2019) p.264.

[116] *Jones* case.

[117] Lawrence Lessing, *Version Code* 2.0 (2006) p.203.

[118] Ibid. p.202.

[119] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others (CCT1/00) [2000] ZACC 12; 2000 (10) BCLR 1079 ; 2001 (1) SA 545 (CC) (25 August 2000).*

warrant authorising a search. In an incidental but important dictum, Justice Langa, delivering the opinion of the court, added the following gloss to the reasonable expectation test of the scope of constitutional privacy:[120]

> 'The right … does not relate solely to the individual within his or her intimate space. Ackermann J did not state …. That when we moved from this established "intimate core", we no longer retain a right to privacy in the social capacities in which we act. *Thus, when people are in their offices, in their cars or on mobile phones, they still retain a right to be left alone by the state unless certain conditions are satisfied*. Wherever a person has the ability to decide what he or she wishes to disclose to the public the expectation that such a decision will be respected is reasonable, the right to privacy will come into play.' [our emphasis]

A court reconsidering this language in a future case where the specific question before it concerns constitutional privacy in the time of digitalisation will have to consider when and whether individuals are able to effectively decide what information to reveal publicly. Under current conditions, much of the collecting, permanent recording and transfer of data occur without the knowledge or even awareness of data subjects. Consent under these circumstances is no more than a fiction. What the courts will demand to enable a meaningful exercise of choice will be a critical constitutional question. So will the nature of the constitutional enquiry into both subjective and objective reasonableness.

The case after *Bester* was also a physical 'search' case under the 'Interim' constitution. In *Mistry v Interim National Medical and Dental Council of South Africa,* the powers of inspection created by the Medicines Act were broad enough to allow inspectors to 'enter any home where aspirins, ointments or analgesics happen to be and once there … [to] inspect not only medicine cabinets or bedside drawers, but also files that might contain a person's last will and testament, private letters and business papers.'[121] In finding that the statutory authority to enter private homes without a warrant and there to rifle through intimate possessions intruded the 'inner sanctum' of persons in breach of their privacy rights, the court held that it was not necessary to decide threshold questions such as what constituted a 'search and seizure.'[122] It did however effectively recognise for the first time in South African law that a constitutional right to informational privacy is 'covered under the broad protection of privacy guaranteed by section 13.'[123] *Mistry* went on to say that whether this privacy right is violated depends on the intrusiveness of the manner the information is obtained, whether it is about intimate aspects of personal life, whether it involved data provided for one purpose which was then used for another, or whether it was disseminated to the press or general public, or to persons from whom there was a reasonable expectation that it would be withheld.[124]

---

120 Ibid. p.16.

121 *Mistry v Interim National Medical and Dental Council and Others (CCT13/97) [1998] ZACC 10; 1998 (4) SA 1127; 1998 (7) BCLR 880 (29 May 1998)* [21].

122 Ibid. p.23.

123 Ibid. p.48.

124 Ibid. p.51.

Although this South African Constitutional Court case did not examine the implications of digitalisation for data collection, processing and dissemination, the influence of the case of the German Constitutional Court[125] which first recognised a personal right to control private information is clear. In that 1983 case, the German Constitutional Court engaged this question directly. In its opinion, 'the individual's decisional authority needs special protection in view of the present and prospective conditions of automatic data processing. It is particularly endangered because…the technical means of storing highly personal information about particular persons is practically unlimited, and information can be retrieved in a matter of seconds with the aid of automatic data processing, irrespective of distance.' As the German court correctly observed, '[t]he possibilities of acquiring information and exerting influence have increased to a degree hitherto unknown and may affect an individual's behavior because of the psychological pressure that public awareness may place upon the individual.'[126]

The final case we will discuss is *AmaBhungane*, the most recent and most important in this context because the Constitutional Court dealt explicitly with the impact of digital technologies on the functioning of the coercive apparatus of the state from a privacy perspective for the first time.[127] It also acknowledged, though this matter was not properly before it, that 'in the age of mass data surveillance, private actors pose a comparable threat to privacy as does the state.'[128] Whether this means that the constitutional right to privacy might well be applied directly to private actors will be interesting to see in the future. It is not clear that there is an existing common law vehicle that can be 'developed', nor does any legislation regulate 'surveillance' by private actors.[129]

AmaBhungane concerned the constitutionality of parliamentary legislation. Under the South African Constitution, determination of this kind of constitutional question takes place in a two-stage enquiry: first, whether a constitutionally protected right has been breached; and second, whether the legislative restriction can be justified under the limitations clause of the Constitution which requires the court to undertake a proportionality analysis.[130]

At stage one, the court dealt with the constitutionality of the Regulation of Interception of Communications and Provision of Communication-Related Information Act[131] under the general right of constitutional privacy in section 14, despite the fact that the section also specifically prohibits 'searches' of one's person and home[132] and protects the privacy of communications.[133]

---

125 The Census Act Case (1983) 65 (B VerFGE 1).

126 See Donald P. Kommers and Russel A. Miller, *The Constitutional Jurisprudence of the Federal Republic of Germany* (3rd edition) pp.409-411.

127 *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).*

128 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) ; 2020 (1) SACR 139 (GP) (16 September 2019)* [111].

129 Regulation of Interception of Communications and Related Matters Act covers state surveillance. POPIA excludes policing.

130 *Bernstein and Others v Bester NO and Others (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996)* (n 62).

131 70 of 2002 (RICA)

132 Section 14(a).

133 Section 14(d).

The adoption of this Act, as the court points out, was 'informed by considerable technological developments in electronic communications' as the legislation authorises 'the interception of both direct and indirect communications, which are defined broadly to include oral conversations, email and mobile phone communications (including data, text and visual images) that are transmitted through a postal service or telecommunications system.'[134] The result is that we do not yet know how a court will deal with 'digital searches' by agencies of law enforcement under section 14 (a) and (b). But of some considerable significance is the fact that the court introduced the concept of 'state surveillance'[135] into its lexicon and analysis. This includes 'searches' by technology. The opening paragraph of the Judgement reads as follows:

> 'The constitution proclaims that "national security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, free from fear and want and to seek a better life." It does so against the *historical backdrop in which the pursuit of a skewed notion of national security was weaponized and calculated to subvert the dignity* of the majority of South Africans. *As part of the pursuit, law enforcement involved searches of people, their homes and belongings*. Over the years, law enforcement evolved to include surveillance of people, their home, their movements, and their communications. *Today technology enables law enforcement agencies to not only physically – as opposed to electronically – invade the "intimate personal sphere" of people's lives, but also to maintain and cement its presence there, continuously gathering, retaining and – where deemed necessary – using the information.*'[136] [Our emphasis]

The first point to be made about the court's rights analysis in terms of the constitutional right to privacy appears from the paragraph quoted above. The court attaches particular importance to constitutional privacy in the light of our experience in South Africa under a 'police state.'[137] 'Axiomatically' it says privacy rights are 'singularly important in South Africa's constitutional democracy.'[138] The court then adds that invasion of an individual's privacy rights infringes the 'cognate right to dignity'[139] which the court has termed elsewhere the 'cornerstone of South African democracy.'[140] The effect of this 'bootstrapping' reasoning is to strengthen privacy protection and to require persuasive justification for state action which invades the right.

It is a short step from here to recognise the particular threats posed by digital policing to constitutional privacy, which is evident in the quoted paragraph above. Yet the court also continues to rely on the *Bernstein* privacy paradigm which affords strong protection to 'intimacy' but works less well as a

---

134 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) ; 2020 (1) SACR 139 (GP) (16 September 2019)* (n 112) para 7.

135 Defined in FN 3.

136 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) ; 2020 (1) SACR 139 (GP) (16 September 2019)* (n 112) para 1.

137 Ibid. p.26.

138 Ibid. p.27.

139 Ibid. p.28.

140 *National Coalition for Gay and Lesbian Equality and Others v Minister of Home Affairs and Others (CCT10/99) [1999] ZACC 17; 2000 (2) SA 1; 2000 (1) BCLR 39 (2 December 1999)* [28].

framework for identifying the threats posed by digital policing to constitutional privacy. The court reasons as follows: 'Imagine how an individual in that situation would feel if she or he were to know that throughout those intimate communications someone was listening in or reading them.'[141] The clandestine interception and surveillance of an individual's communications is therefore 'violative of an individual's inner sanctum' and 'a highly and disturbingly invasive violation of privacy.'[142] But is surveillance and monitoring, with our knowledge, of communications which are not 'intimate' less disturbing and invasive? The court appears to recognise potential problems with its reasoning, which arise from the impact of digitalisation on the boundary between the private and the public, or as Lessig would term it 'privacy in public'. It acknowledges that the Act:

> 'allows interception of *all* communications. The sanctioned interception does not discriminate between intimate personal communications and communications… *privacy is breached along the entire length and breadth of the "continuum". And this intrusion applies equally to third parties* who are not themselves subject to surveillance…' [our emphasis]

After finding that there can be no question that 'surveillance of private communications limits the right to privacy', the court went on as required to consider whether the limitation is 'reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.'[144'145] It is at this second stage that some of the main elements emerge of the court's reasoning in upholding the High Court's declaration of unconstitutionality of the basic structural elements of 'the Act'. In essence it said that the Act does not pass the test of constitutionality because its design features fell short of what the Rule of Law requires, in that the Act failed to provide safeguards for independent judicial supervision and for the notification of subjects of surveillance; in that it allowed the police to seek permission for interception *on ex parte* application without adequate safeguards; in that it failed to provide adequate procedures to ensure that data obtained through surveillance is managed lawfully; and it failed to provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist.[146] The rule of law also informed the court's conclusion that unregulated, untargeted 'bulk surveillance' of all information is 'an extreme violation of privacy … in violation of comparative and international law.'[147] It is clear therefore that the court in this case relied on its proportionality analysis to impose strong rule of law constraints on state surveillance, thereby subjecting systemic aspects of the system of surveillance to constitutional standards.

---

[141] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) ; 2020 (1) SACR 139 (GP) (16 September 2019)* (n 112) para 23.

[142] Ibid. pp.23–24.

[143] Ibid. p.24.

[144] Ibid. p25.

[145] Section 36.

[146] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) ; 2020 (1) SACR 139 (GP) (16 September 2019)* (n 112) para 157.

[147] Ibid. p.129.

Of the four Constitutional Court cases discussed above, only the most recent, *AmaBhungane*, engages with the consequences of digitalisation, ruling mass surveillance out of bounds in terms of the constitutional right of privacy. While on a superficial reading the earlier cases of *Bester, Hyundai Motor Distributors,* and *Mistry* would not appear to offer much to those concerned with the dangers posed to privacy by digitalisation, our reading of them as based on dignity rather than narrowly on liberty has emphasised the links and the potential these types of cases have to safeguarding the concept of privacy in public and to the right of information privacy. Responding to the facts and arguments presented, the cases (except *AmaBhungane* only cursorily) have not to date grappled with the difficult issues of private power. But, taken as a whole, South Africa's decided privacy jurisprudence demonstrates how the constitutional elements of rights and proportionality analysis, as well as constitutional supremacy, have laid a good foundation for continued engagement with future state surveillance practices.

(b) Publication, dissemination and use

Before the adoption of the 1996 Constitution and the section 14 constitutional right to privacy, and before the 'Interim Constitution' was introduced, the South African legal system recognised a right to privacy as an independent personal right under the common law of delict, the *actio iniuriarum*. Judicial authority for this proposition is the *O'Keeffe*[148] case which in 1954 extended the action to include a cause of action for the publication of private facts. The case concerned an unauthorised publication of a person's photograph for advertising purposes.

In this context, the main importance of the *actio* has been in affording some protection to individuals against the excesses of the mass media. In *Financial Mail (Pty) (Ltd.) v Sage Holdings Ltd.*[149] the Appellate Division, the highest court in the country at the time, clarified that a breach of privacy under the common law could occur either by unlawful intrusion upon the personal privacy of another, or the unwanted disclosure of private facts that a person has a right to conceal. In his taxonomy of the common law right to privacy, Professor David McQuoid-Mason adds,[150] placing a person in a false light by publishing non-defamatory but false statements, and the misappropriation of a person's image or likeness without consent or permission. It has been suggested that the latter is more properly considered as a breach of the separate right to an identity.[151] However, in *Bernstein*, Justice Ackermann pointed to the close relationship between privacy and 'what is necessary to have one's own autonomous identity.'[152] In agreement with McQuoid-Mason, the Supreme Court of Appeal extended protection to features of a person's identity in *Grutter v Lombard* under the

[148] *O'Keeffe v Argus Printing and Publishing Co. Ltd.* 1954(3) SA 244 (C).

[149] *Financial Mail v Sage Holdings Ltd.*

[150] David McQuoid-Mason 'Invasion of Privacy: Common Law v Constitutional Delict' 2000 *Acta Juridica* 227 citing Prosser's 1960 article.

[151] Neethling, Potgieter and Visser *Law of Delict* (n 4) p.284.

[152] *Bernstein and Others v Bester NO and Others (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996)* (n 62) para 65.

actio iniuriarum.[153] Appropriation of an individual's image or likeness for the benefit of another, or for commercial purposes and without consent, therefore constitutes an actionable breach of privacy rights under both the South African common law *and the constitution*, a point we come back to below.[154]

We propose that a full specification of the public law perspective on privacy should identify the potential of the four privacy delicts (intrusion, disclosure, false light and appropriation) recognised under the South African common law to provide protection against the specific harms associated with digitalisation. As we have pointed out, digitalisation magnifies the risks of 'data spillages' and uses and abuses of personal information harmful to the privacy of individuals in ways that could not have been imagined in Brandeis's world of the hand-held camera.[155] While the detail must await further research, we can offer a high-level answer here. The answer is some protection – but that the conceptual structure of the law of delict designed to remedy specific, discreet and quantifiable harms does not reach the 'systemic issue of power' or the 'aggregation problem' as Solove points out.[156] They are all furthermore currently cast in the paradigm of concealment and secrecy.[157] The delict of 'intrusion' for instance can provide only limited protection in the face of the consolidation of public records in centralised databases, and the collection and dissemination of information in 'cyberspace' which is a 'public space.' However, we do not yet know how the Constitutional Court will use its powers to develop the common law in response to digitalisation, and whether it will recognise a new 'constitutional delict' for the breach of privacy rights as proposed by Prof. McQuoid-Mason.[158] Our view, which aligns with McQuoid-Mason's and is open to exploring the possibilities of developing the common law of delict within a constitutional framework, also finds some support in the argument recently made by our colleague, Emile Zitzke.[159] Zitzke was reflecting on the award for damages made in a high-profile matter concerning egregious failures by the Gauteng Department of Health for the care of mental health patients. Zitzke asks whether constitutional damages as opposed to the 'old' version of the common law was the appropriate vehicle to consider what remedy would be 'just and equitable' in this case.

The two delicts with the greatest potential, in our view, are the appropriation delict and disclosure of private facts delict. Under a public law paradigm and a transformative constitution, it is difficult to see why the sale of personal information collected from users or purchased as a commodity cannot potentially give rise to liability, at least where there is a 'spillage'. The disclosure of private

---

153 *Grütter v Lombard and Another (628/05) [2007] ZASCA 2; [2007] 3 All SA 311 (SCA); 2007 (4) SA 89 (SCA) (20 February 2007).*

154 Ibid. p.9.

155 Op. cit. Omri. These 'data emissions', which are increasingly leaked into the digital ecosystem, are harmful to private and individual interests. They also disrupt the functioning of social and political institutions in ways that are harmful to the public interest. This points to the limits of privacy law, particularly in the form of tort law. But we can see no reason why an individual who has suffered demonstrable harm should not be able to recover damages under the common law or under a newly minted 'constitutional delict'.

156 Solove, 'Privacy and Power: Computer Bases and Metaphors for Information Privacy' *Stanford Law Review* (2001) vol. 154 at 1434.

157 Ibid. p. 1439.

158 Invasion of privacy.

159 Zitzke, Emile, 'The Life Esidimeni Arbitration: Towards transformative constitutional damages?', *Journal of South African Law / Tydskrif Vir Die Suid-Afrikaanse Reg* 2020, no. 3 (July 1, 2020): 419–40, https://hdl.handle.net/10520/EJC-1e43fc18fa [accessed on 02 June 2021].

facts delict has thus far primarily been invoked against traditional mass media. But who is the media today? And what constitutes 'publication' in the time of digitalisation? We increasingly rely on social media companies to communicate and on 'Big Tech' platform companies that aggregate and sell our personal data for information and news. This is why Jack Balkin has suggested that they should be regarded as 'information fiduciaries' that should be held to higher legal and ethical standards than they are at present under US First Amendment law.[160]

It is becoming clear that these monopolies can (and do) exercise control over content and therefore effectively act as custodians of the 'virtual public square'. But, under South African law, it is not clear whether they can attract liability as do other media companies for the 'publication' or inadvertent disclosure of private facts or defamatory statements under the *actio iniuriarum*. Section 73 of the Electronic Communications and Transactions Act[161] immunises internet service providers that are 'mere conduits' from liability for 'providing access to, or for operating facilities for information systems, or for information systems or transmitting, routing or storage of data messages.' As far as we are aware, there is as yet no South African case in which monopolistic platform companies or other web-based 'publishers' have been sued under the common law. However, individuals who post material are treated as publishers and can be held liable under the common law. This is what happened in the recent case, *Economic Freedom Fighters and Others v Trevor Manuel* in which a former minister successfully sued members of a political party under the common law for delictual damages for posting defamatory statements about him on Twitter.[162] The corporation owning the digital platform was not cited as a respondent. But what of other kinds of harms to privacy that result from digital processing of personal information or result from 'publication' of such information on digital platforms? Or from the 'spillage' of personal information? And can the platforms themselves be held liable? This question, in turn, implicates the issue of the design of intermediary liability rules in South Africa. Indeed, what constitutional standards can and should they be held to? These are questions that have not yet been answered in South Africa. But we think that there exists within our system of constitutional democracy considerable normative and institutional resources to develop what we have called a public law paradigm that is responsive to the risks to privacy and other rights in age of 'digitalisation plus'.

[160] Op. cit. Balkin.

[161] Act 25 of 2002.

[162] *Economic Freedom Fighters and Others v Manuel (711/2019) [2020] ZASCA 172; [2021] 1 All SA 623 (SCA) (17 December 2020).*

Part Five: Conclusion

Intervening in a set of rapidly evolving debates occurring at both global and national levels, this working paper has asked what legal resources are available in the South African legal system to respond to the risk and benefits posed by digitalisation.

In addressing the question, we have made three arguments. First, we have argued that this question is best answered through the lens of 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. In particular, our public law perspective would reframe privacy law as *both* a private and a public good essential to the functioning of a constitutional democracy in the era of digitalisation.

Second, we argued 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. This view takes into account the adoption of South Africa's 'transformative constitution', with particular characteristics, including the components of horizontality (e.g. the application of constitutional norms to both public and private actors) and of subsidiarity.

Our third and final argument was built on a discussion of the Constitutional Court's case law on the right of constitutional privacy, dividing that discussion into the recent Constitutional Court cases addressing surveillance harms and those resolving disputes addressing the harms associated with publication, dissemination, and use. We argue that constitutional privacy jurisprudence in South Africa has not explicitly confronted the implications of impacts of disruptive technological change (until recently). Nonetheless, it has demonstrated potential to do so. We have acknowledged the creative potential of proportionality/rule of law analysis to focus simultaneously on the need for systemic controls of harms to privacy and democracy and to recognise the need to incorporate an assessment of the need/benefits for sectors such as law enforcement and social rights in the constitutional analysis.

Delving into one particular national context, in developing our public law perspective, we have argued that the South African constitutional framework provides rich resources for developing a constitutional right of privacy at least roughly adequate for the challenges posed by the current era of digitalisation plus.

The answers to foundational questions of great import for our society and community cannot be crowdsourced in milliseconds. But we do hope this paper contributes to this ongoing and multi-layered conversation of democratic self-government in the age of digitalisation.


BLAVATNIK
SCHOOL OF
GOVERNMENT
UNIVERSITY OF
OXFORD


Digital
Pathways
at Oxford