

https://dspace.org/

Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization

Firoz Cachalia; Jonathan Klaaren

CAMBRIDGE UNIVERSITY PRESS
https://hdl.handle.net/10539/40210
WOS

Downloaded from a DSpace repository. https://dspace.org/

Journal of African Law (2024), **68**, 89–107
doi:10.1017/S0021855323000268

RESEARCH ARTICLE

Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization

Firoz Cachalia* and Jonathan Klaaren**

University of the Witwatersrand, Johannesburg, South Africa
Corresponding author: Jonathan Klaaren, Email: Jonathan.klaaren@wits.ac.za

(Accepted 9 January 2023; first published online 6 November 2023)

Abstract
Rapid and radical digitalization and the "fourth industrial revolution" are generally associated with progress, but also pose significant risks to privacy rights and democracy. This article proposes a public law reading of the South African Constitution to respond to the dangers posed by disruptive technological change, in light of the constitution's rights-orientated and rule-of-law-centred approach to interpreting the right to privacy. It examines the legal resources available in the South African legal system and, specifically, its constitution. The article emphasizes the way South African privacy jurisprudence infuses the right to privacy with the value of dignity, and how this allows an interpretation that sees privacy as a public, as well as private, right. The article concludes that this rights jurisprudence, alongside the constitutional principles of proportionality, subsidiarity and supremacy, has established a working foundation to articulate the right to privacy in a way that is suitable in the digital age.

Keywords: Privacy; digitalization; public law; transformative constitutionalism

Introduction

Klaus Schwab, founder and executive chairman of the World Economic Forum, has characterized the current phase of "digitalization" (involving a much more ubiquitous and mobile internet, smaller more powerful and cheaper sensors, artificial intelligence and machine learning) as a "fourth industrial revolution".[1] This distinguishes this phase of rapid and disruptive technological change from earlier iterations.[2] For Schwab, the combination of information technology, artificial intelligence and biotechnology heralds the possibility of integrating the physical and virtual worlds, the biological body and machines in a post-human world. This change and its possibilities raise some fundamental questions about the way we understand ourselves and the way we organize our societies, economies and polities. The most basic commitments of constitutional democracy to individual agency and collective self-determination may now be threatened by disruptive technological change.[3]

While the dominant narrative is "digitalization as progress", there is another critical view, emerging especially in universities and civil society, which presents an alternative to this sunny

* Adjunct professor of law and director, Mandela Institute, University of the Witwatersrand, Johannesburg.
** Professor of law, University of the Witwatersrand, Johannesburg.

1 K Schwab *The Fourth Industrial Revolution* (2017, Penguin) at 7.

2 Digitalization (the storing of information in digital as opposed to analogue or paper-based forms) has had social and economic impacts since at least the 1960s. The pace and depth of these impacts has increased since the middle of the first decade of this century. Many speak now of a process of digitalization as a social and economic process in its own right. See A Appadurai and N Alexander *Failure* (2019, Wiley).

3 Schwab *The Fourth Industrial Revolution*, above at note 1 at 46.

© The Author(s), 2023. Published by Cambridge University Press on behalf of SOAS University of London. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

perspective and sees "digitalization as progress" as being informed by an uncritical teleology that underestimates its potential costs. Evaluations of "digitalization as progress" are deeply rooted in the cultural and intellectual history of industrializing societies, which in the West is associated with the Enlightenment and the birth of modernity. 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,[4] and so too the fourth iteration. However, in the authors' view, the costs (which include, but are not limited to, privacy costs) must also be considered in fashioning a long-term regulatory and policy response to technological change. Recent incidents and trends (such as Edward Snowden's revelations about secret mass surveillance by the US National Security Agency, public disclosure that social networking platform Facebook had sold data to shape voter preferences and influence the outcome of ostensibly democratic elections, and the understanding of how technology platform companies track our online lives to attract advertising revenue and monetize personal data) call into question the simple association of digitalization with linear progress.

In addition, while Schwab's "digitalization as progress" story accurately presents digitalization as a global process, this process has differing impacts within states and is perhaps primarily responded to at the national level. This article focuses specifically on the response of the South African legal system to technological change. South Africa faces many socio-economic challenges arising from its apartheid legacy and its subordinate positioning in the global economy, yet, as a constitutional democracy, it must also face up to many contemporary "wicked problems"[5] including those associated with the fourth industrial revolution.

The critical perspective argues that South Africa is either in danger of becoming a surveillance state or has indeed already partially become one.[6] In 2018, Jane Duncan, a professor of journalism, commented that "[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".[7] The UN Human Rights Committee has 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."[8]

4 See CB Frey *The Technology Trap: Capital, Labor and Power in the Age of Automation* (2019, Princeton University Press).

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, NISC Pty Ltd). "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.

6 K Breckenridge "The biometric state: The promise and peril of digital government in the new South Africa" (2005) 31/2 *Journal of Southern African Studies* 267; *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* 2021 (3) SA 246 (CC).

7 J Duncan *Stopping the Spies* (1st ed, 2018, Wits University Press) at 221.

8 Human Rights Committee "Concluding observations on the initial report on South Africa", CCPR/ZAF/1 (2016), paras 42–43.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

With attention to the largely positive discourse on digitalization's potential impact on South African society and caution about its costs, the authors embark in this article on the development and illustration of their public law perspective on constitutional privacy. The article asks what legal resources, embodied in various legal instruments (such as the doctrines and concepts of constitutional rights, proportionality, horizontality and subsidiarity), are available in the South African legal system post-1994 to respond to the risks and benefits of digitalization. It explores this question from a "South African public law perspective", focusing on the constitutional debates and case law regarding the right to privacy, adopting a method that is largely theoretical. The development of this perspective has been enabled by a "transformative constitution" with particular characteristics, including the component of horizontality, under which constitutional norms apply to both public and private actors. This contrasts sharply with the pre-1994 position in the South African polity where privacy was solely a private law, common law or delictual matter.

This perspective highlights questions of legal ordering that necessarily engage the normative foundations of constitutional democracies. 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 him/herself?

This perspective does not ignore the benefits of digitalization, but is sceptical of the claims of the autonomous functioning of digital technologies and their supposedly benign transformative purposes. The article focuses 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, "[b]y 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".[9]

The authors therefore postulate the need for the development of a public law perspective on privacy, particularly one grounded in constitutional norms. It must: 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;[10] situate this reconsideration of privacy law in the context of the harms, risks and power dynamics[11] generated by digitalization and the way these technologies are being used by governments and the private sector;[12] and examine the balances to be struck between the costs and benefits of digitalization in a constitutional democracy with its particular set of commitments to both individual and collective self-determination, and to the rule of law.

The first part of the article develops and articulates a theoretical perspective that informs a public law perspective on constitutional privacy in the era of digitalization, by discussing privacy law contextually in relation to state power, the logics of surveillance capitalism and the functioning of constitutional democracies. It then turns more explicitly to legal frameworks and considers the constitutional right to privacy in the context of South Africa's transformative constitutionalism and its potential to respond to the harms of digitalization. The authors argue that the South African Constitution of 1996 (the Constitution) instantiates a rights-orientated and rule-of-law-centred political theory that 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. After surveying transformative constitutionalism, private power and constitutional privacy,

9 J Sadowski *Too Smart: How Digital Capitalism Is Extracting Data, Controlling Our Lives and Taking over the World* (2020, MIT Press).

10 C Veliz *Privacy is Power: Why and How You Should Take Back Control over Your Data* (2020, Penguin Random House) at 27.

11 Sadowski *Too Smart*, above at note 9 at 38.

12 L Lessig *Code: 2.0* (2006, Basic Books) at xv.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

the article discusses the case law of the Constitutional Court (the Court) on the right to constitutional privacy.

Towards a public law perspective on constitutional privacy in the era of digitalization

This section considers: privacy law; the state and capital; and the interaction of democratic self-government and privacy.

Digitalization 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[13] in which they proposed that privacy should be recognized as a specific delictual right in light of the harms to individuals created by new technologies, like hand-held cameras.[14] In their articulation, this was a "right to be left alone".[15]

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, machine learning, data mining and predictive analytics. An article of Daniel Solove's, 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: information collection; information processing; information dissemination; and invasion.[16]

Solove's taxonomy can, for the most part, accommodate an analysis of the risks to privacy in the current period of accelerated digitalization, but with some modifications. The amplified risk associated with digitalized "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 volumes of information across data sets by numerous public and private organizations.[17] Solove also anticipates the harms associated with decision-making concerning the "digital person" based on pooled data from many data sources. However, he does not specifically discuss the harms related to data mining and predictive analytics increasingly relied upon by public organizations to allocate public benefits and by private commercial organizations to monitor the preferences and behaviours of their customers. In this regard, Sandra Wachter and Brent Mittelstadt have recently usefully argued that the 2018 EU General Data Protection Regulation 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 a new data protection right to "reasonable inferences".[18]

Soloves's taxonomy also usefully recognizes the structural impact of state surveillance (enabled by the new digital technologies) on power dynamics between states and individuals.[19] But his focus on the harms to the individual misses the systemic and collective nature of privacy harms that is now

13 SD Warren and L Brandeis "The right to privacy" (1890) 4/5 *Harvard Law Review* 193.

14 Id at 195.

15 Ibid.

16 DJ Solove "A taxonomy of privacy" (2006) 154/3 *University of Pennsylvania Law Review* 488.

17 O Ben-Shahar "Data pollution" (2019) 11 *Journal of Legal Analysis* 105, which challenges the view that the injuries from "digitalization 2.0" are exclusively private, arguing that personal information shared in the digital economy undermines and degrades public goods and interests, and therefore that legal framings (like privacy and tort law) that assume that harms are exclusive to individual interests are inadequate.

18 S Wachter and B Mittlestadt "A right to reasonable inferences: Rethinking data protection law in the age of Big Data and AI" (2019) 2 *Columbia Business Law Review* 494.

19 Veliz *Privacy is Power*, above at note 10 at 499.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

becoming evident. As Carissa Veliz notes, "[p]rivacy is not only about you … [p]rivacy is as collective as it is personal … privacy resembles ecological issues and other collective action problems".[20] That your data is personal seems to imply that you are the only concerned party when it comes to sharing it, but this is not necessarily the case[21] as, for example, the sharing of genetic information can impact on others in a family group.

These externalities and information asymmetries have important implications for how we think about the harms and risks to which privacy law must respond today. They call 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".[22] Data protection itself may implicate other rights beyond privacy, such as equality and dignity.

The addition of a group of activities potentially harming our social and collective existence through their systemic impact (akin to Solove's item of "invasion" but without its individualistic conceptualization) would be a valuable modification to his typology of potentially harmful groups of activities. The following sections 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.

Digitalization 2.0: The state and capital

Solove's 2006 analysis of the privacy harms that arise from the information practices of public authorities also pays insufficient attention to the way digitalization 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 digitalization must be situated within the context of the political economy of what can be termed "surveillance capitalism"[23] or "digital capitalism".[24]

The modern bureaucratic state apparatus has always had to map its subjects and citizens systematically, by gathering and recording information in order to carry out its public functions.[25] Even those holding a restrictive view of the state's economic and social functions accepted the Hobbesian[26] view that the state had to provide security and that its policing powers had to include powers of search and seizure.[27] Digitalization exponentially expands the contemporary state's bureaucratic powers of computation, control[28] and surveillance, leading some scholars to turn to Foucaudian concepts such as biopower and disciplinary power to examine the way digitalization is fundamentally restructuring power relations between individuals and the state: "[t]he 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".[29]

20 Id at 75.
21 Id at 76.
22 J Bridle *New Dark Age: Technology and the End of the Future* (2019, Verso Books) at 2.
23 S Zuboff *The Age of Surveillance Capitalism* (2019, Profile Books).
24 Sadowski *Too Smart*, above at note 9.
25 R Lucas "The surveillance business" (2020) 121 *New Left Review* 132.
26 Id at 140–41.
27 US Constitution, Fourth Amendment.
28 G Deleuze "Postscript on societies of control" (May 1990) 1 *L'Autre Journal*.
29 Sadowski *Too Smart*, above at note 9 at 41. See also Veliz *Privacy is Power*, above at note 10, chap 3.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

Law enforcement agencies in many countries are also increasingly relying on "big data" to investigate crime, as well as on dragnet surveillance technologies like CCTV cameras, GPS locational technologies and drones purchased from companies manufacturing the high-tech tools for "smart policing".[30] Such technologies operate at a wholescale or systemic, rather than individual, level. These capabilities are of undoubted value in combatting sophisticated organized crime and transnational crimes such as money laundering. However, pervasive, systemic surveillance comes at a substantial cost to privacy and the freedoms that are essential to our ability to function and flourish as 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.[31] Also, under South African law, law enforcement agencies have not been required to observe the statutory processing rights of data subjects and so are not constrained by principles of data minimization when investigating actual crimes or even suspected criminal conduct.[32] Digitalized surveillance and crime investigation techniques based on data analytics obviously raise some important questions about the adequacy of search and seizure privacy laws, premised on a now-obsolete conception of a spatial boundary between public and private space.

To situate the threats to privacy (threats to the functioning of constitutional democracies in the digital age) properly, it is necessary to focus on these accretions of state power, as well as on the "logic of accumulation" in the age of surveillance capitalism:[33] ownership of the "means of behavioural modification eclipses ownership of the means of production as the fountainhead of capitalist wealth and power in the 21st century".[34] Consciously invoking Marx, Shoshana Zuboff shows how an extractive economic logic has developed on the infrastructural backbone of smart computing, which instrumentalizes the most human and personal experiences to the commercial ends of platform companies and turns personal data into capital.[35] 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.[36] 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 conceptualization 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.[37] The harms associated with private commercial power must also be reckoned with.

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 systems 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

30 Sadowski, ibid.

31 Right2Know Campaign and Privacy International Report to the 27th Session of the UN Human Rights Committee on the Right to Privacy in South Africa (2016), paras 41–45.

32 Ibid.

33 Zuboff *The Age of Surveillance Capitalism*, above at note 23.

34 Id at 12. For a critique of aspects of this argument, see K Breckenridge "Capitalism without surveillance?" (2020) 51/3 *Development and Change* 921.

35 Sadowski *Too Smart*, above at note 9 at 40.

36 A Berlin court ruled that Facebook's privacy settings violate consumer and data protection laws, under the German Competition Act, sec 32.

37 L Tribe *The Constitution in Cyberspace: Law and Liberty beyond the Electronic Frontier* (1991, American Humanist Association). Tribe defends the limited reach of the US Constitution in the form of the "state action doctrine".

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

technologies, which have facilitated the dissemination of polarizing propaganda and false information. Reliable procedures for arriving at agreement on the facts by public deliberation are essential to the functioning of democratic societies that aim to structure conversation among a variety of opinions and interests. The capabilities enabled by digitalization have also weakened the mass media and political parties, and represent a real danger to the integrity of elections: the evidence is now clear that voter preferences can be manipulated through targeted advertising and psychological profiling.[38] The accretions of private power associated with digitalization and their intersection with public power are also accentuating underlying tendencies towards plutocracy and oligarchy in constitutional democracies today.[39] This undermines the claims of their systems of authority based on popular consent and political equality.

Therefore, the capabilities enabled by digital technologies and the power dynamics that have been unleashed require reinvigoration of a commitment to individual self-determination as well as to democratic self-government, and recognition of their interdependence. Under a public law paradigm, privacy today is much more than a negative individual right[40] 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 current pervasive system of surveillance, we need a richer concept of the constitutional value of privacy in constitutional democracies, instead of merely the right "to be left alone". Privacy must be understood as being integrally related to individual autonomy and agency.[41] In *Bernstein v Bester*, the first privacy case in South Africa in the post-apartheid era, Ackermann J 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".[42]

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, without the constant external pressure of being watched, profiled and assessed by the state and commercial entities.[43]

Transformative constitutionalism and the constitutional right to privacy

What textual and interpretive resources are there under the Constitution to develop a public law perspective on privacy law that is responsive to the harms associated with the current stage of digitalization? This article argues that the South African constitutional text instantiates a rights-orientated and rule-of-law-centred political theory that potentially facilitates the development of a constitutional law of privacy that is more suited to the digital age.

Judicial review, constitutional rights and the principle of proportionality

There are two important but unremarkable ways in which the text of the Constitution augments the conceptual resources available for judicial reasoning in the field of South African privacy law. The first is that it entrenches (as do many modern constitutions and human rights instruments)[44] a

38 Veliz *Privacy is Power*, above at note 10 at 102.

39 F Cachalia "Precautionary constitutionalism, representative democracy and political corruption" (2019) 9 *Constitutional Court Review* 45.

40 I Berlin *Two Concepts of Liberty* (1969, Oxford University Press).

41 Veliz *Privacy is Power*, above at note 10 at 72.

42 *Bernstein and Others v Bester NO and Others* 1996 (2) SA 751 (CC), para 65.

43 Veliz *Privacy is Power*, above at note 10 at 72.

44 For example, the International Covenant on Civil and Political Rights, art 17 and European Convention on Human Rights, art 13. The African Charter of Human and Peoples' Rights does not expressly protect privacy rights.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

constitutional right to privacy. Section 14 of the constitutional Bill of Rights provides: "[e]veryone 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."

It is important to note that the post-apartheid introduction of the Bill of Rights by no means extinguished the common law on the right to privacy, which continues as part of the South African legal system, albeit controlled by the Constitution as the supreme law. In addition, privacy legislation (which came fully into effect in mid-2021) created a statutory right to privacy and established a regulator for privacy rights, also with jurisdiction over the constitutional right of access to information.[45]

Secondly, beyond the entrenchment of this fundamental right to privacy, 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, under section 7(2), the state is required to "respect, protect, promote and fulfil". The Bill of Rights applies to all law and conduct,[46] and binds the legislature, the executive and the judiciary.[47] Section 167 concentrates the power to decide questions of constitutionality in the Court. This includes parliamentary legislation[48] and "all law", which must comply with the rights provisions of the Bill of Rights and the founding value of the rule of law.[49] The Constitution can therefore be understood to establish 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.

In this fashion, the constitutional text already 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 digitalization. Furthermore, the Bill of Rights also includes other fundamental rights, such as the rights to equality[50] and dignity,[51] which can support the development of a public law perspective. In a case concerning an action for defamation against a media company under common law, Kate O'Regan J said the following about the symbiotic relationship between the constitutional right to privacy and another constitutional right, the right to dignity:

> "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 14 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."[52]

The core constitutional value of dignity works in two ways: reinforcing privacy as a liberty that protects intimacy and individual choice from interference by the state or third parties; and recognizing and protecting an individual's interest in public estimations of an individual's worth. This conception has the potential to reach the harms associated with digitalization that are much less plausibly

45 F Cachalia and J Klaaren "Digitalisation in the health sector: A South African public law perspective" (2022) 25 *Potchefstroom Electronic Law Journal* 1 at 4.
46 The Constitution, sec 2.
47 Id, sec 8.
48 Id, sec 167(b).
49 Id, sec 2.
50 Id, sec 9.
51 Id, sec 10.
52 *Khumalo and Others v Holomisa* 2002 (5) SA 401 (CC), para 27.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

conceptualized as intrusions in protected spaces or individual decisions, including 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.[53]

Constitutional rights to privacy and dignity in the Constitution are "strong" rights that cannot simply be weighed against some supposed public benefit.[54] They can only be limited in accordance with principles of proportionality expressly set out in section 36 of the Constitution itself. This limitation clause provides:

> "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 examine carefully both the ends and means of legislative decisions in light of the constitutional commitment to privacy and dignity. Mere utilitarian balancing of costs and benefits is obviously excluded.

Constitutional supremacy, subsidiarity and horizontality

The Constitution has distinctive features of subsidiarity and horizontality that further enhance the potential for constitutional law to respond to technological change. In its continued development of these doctrines in the "digitalization plus" age, the Court will have to stay abreast of rapidly changing technologies and shoulder much of the responsibility for the constitutional response.

The doctrine of subsidiarity consists in South Africa of the founding principle of constitutional supremacy,[55] read with its correlate, the judge-made rule of subsidiarity. Parliamentary legislation must comply with constitutional norms to be valid. The legal norms created by legislation are therefore subsidiary ones. Where the wording of a constitutional right requires that the legislature give effect to the constitutional right,[56] 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

53 See JQ Whitman "Two western cultures of privacy: Dignity vs liberty" (2004) 13 *Yale Law Journal* 1151 on the protection of personality rights under German privacy law and the importance attached to the value of dignity.

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

55 The Constitution, sec 1 provides that the country is one sovereign, democratic state founded on the supremacy of the Constitution and the rule of law.

56 For example, the right to lawful, reasonable and procedurally fair administrative action in sec 33. J Klaaren "Constitutional authority to enforce the rights of administrative justice and access to information" (1997) 13 *South African Journal on Human Rights* 549.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

right.[57] However, the Court has effectively embellished the statutory right with a constitutional gloss by insisting that a statutory right has to be interpreted in light of the norms of the more abstract constitutional right.[58] 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; this 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 and as noted above, giving at least partial effect to the constitutional right to privacy, Parliament enacted a privacy law in the form of data protection legislation, the Protection of Personal Information Act 2013 (POPIA).[59]

In a fascinating and significant case in January 2021, the 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 NO and Others v De Jager and Others*,[60] the Court had to decide 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 as the statutory framework did. 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. Most interestingly for our purposes here, Victor AJ, concurring with the majority, wrote separately to argue for a more direct and robust application of the Equality Act on the basis of subsidiarity:

> "Evidently, 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'".[61]

While the authors' public law perspective aligns with that of Victor AJ, there is one crucial difference between that equality question and the privacy-centred topic: the scope of the legislation enforcing the constitutional right or at least some part of it. In the authors' view, Parliament's recently enacted privacy legislation does not cover the whole field of the constitutional right to privacy.[62] POPIA is an important statute with a significant role, but it does not even claim to treat the full

57 *My Vote Counts NPC v Speaker of the National Assembly and Others* (CCT121/14) [2015] ZACC 31; *My Vote Counts NPC v Minister of Justice and Correctional Services and Another* 2018 (5) SA 380 (CC); R Cachalia "Botching procedure, avoiding substance: A critique of the majority judgment in *My Vote Counts*" (2017) 33 *South African Journal on Human Rights* 138; J Klaaren "My Vote Counts and the transparency of political party funding in South Africa" (2018) 22 *Law, Democracy, & Development* 1; M Murcott and W van der Westhuizen "The ebb and flow of the application of the principle of subsidiarity: Critical reflections on Motau and My Vote Counts" (2015) 7 *Constitutional Court Review* 43.

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

59 The Court has assumed that a right to information privacy exists under POPIA, sec 13: *Mistry v Interim National Medical and Dental Council and Others* 1998 (4) SA 1127, paras 47–48. It thus remains arguable that an alternative or supplemental text for a right to informational privacy is found in 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: J Klaaren "The right of access to information at age ten" in *Reflections on Democracy and Human Rights: A Decade of the South African Constitution* (2006, South African Human Rights Commission) 167.

60 2021 (4) SA 1 (CC).

61 Id, para 190.

62 The right to privacy does not cover all the constitutionally cognizable harms associated with digitalization. Decision-making by algorithm will raise other challenges, and discriminatory decisions could, for instance, be challenged on equality grounds, as well as on unfair or unreasonable grounds, under the right to administrative justice.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

scope of questions of interest exhaustively. While it is not the purpose of this article to answer them, clearly questions about the relationship between the constitutional right to privacy and the statutory rights and structures created by POPIA will arise. Although POPIA defines "personal information" and "processing" very broadly, it does not cover all the privacy harms associated with digitalization, particularly surveillance and dissemination harms, as identified above.[63] The authors thus argue that section 14 of the Constitution will therefore continue to occupy a (if not the) central place in the development of South Africa's privacy jurisprudence in response to technological change.[64]

The Constitution also explicitly confers law-making powers on the Court by empowering it 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 as privately owned companies are an integral part of the political economy of 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 common law rules to limit the right in accordance with the constitutional limitation clause. We have already seen that no legislation 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) of the Constitution 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 Chaskalson J observed: "[t]here 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".[65] 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 that has received little attention until recently.[66]

Transformative constitutionalism, private power and constitutional privacy

The text of the Constitution has certain unique provisions that distinguish South Africa's version of the constitutionalist ideal from the "classical" version in the balance it strikes between "conservation" and social change. One particularity 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 Constitution's transformative potential could be unlocked if the judiciary abandoned formalist interpretive practices and recognized the imperative to contribute to the realization of the political

63 POPIA, sec 6 excludes data processing for law-enforcement purposes, but only to the extent that adequate safeguards for the protection of personal information have been established in other legislation. Such envisaged legislation has not yet been enacted. Id, sec 7 excludes journalism.

64 See A Roos "Privacy in the Facebook era: A South African legal perspective" (2021) 129/2 *South African Law Journal* 375.

65 *Pharmaceutical Manufacturers Association of South Africa and Another: In re Ex Parte President of the Republic of South Africa and Others* 2000 (2) SA 674, para 44.

66 A debate over the content of an African conception of privacy has recently spilled into the pages of scholarly journals, which raises a question beyond the scope of this article: whether there exist specifically African notions of privacy that 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. See AB Makulilo "The quest for information privacy in Africa" (2018) 8 *Journal of Information Policy* 317.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

project instantiated in the text by adopting a "post liberal" theory of adjudication.[67] 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".[68]

The main focus of the work of the generation of scholars who enthusiastically embraced Klare's work was on expansive readings of equality[69] and socio-economic rights,[70] not constitutional privacy. However, the two sets of provisions that Klare identified in making his case for transformative constitutionalism will certainly be relevant to the development of South Africa's law of privacy in the digital age: section 7(2), which imposes affirmative duties on the state; and section 8(2) and (3), which extends the application of the Constitution's rights provisions to private relationships regulated by common law and thus potentially directly to private power.

Klare's characterization of the 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[71] and whether transformative constitutionalism requires judicial interpretive practices informed by critical legal theory. Theunis Roux[72] has argued that the progressive purposes of the Constitution (for which he agrees there is ample textual evidence) can just as easily be realized by conventional adjudicative practices informed by a Dworkinian[73] conception of the political morality that should inform constitutional reasoning. In this context, the authors agree with Roux to this extent: rights and rule-of-law constitutionalism provide rich resources for the development of privacy rights protection. However, for the Court to develop a harm principle in the field of privacy rights, the authors think 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 does Dworkin's to judicial interpretive practices that incorporate consideration of the implications of power relations, which a public law perspective on constitutional privacy must take account. This raises questions about the boundaries of constitutional law as an interpretive practice. For example, can constitutional law not function more like competition law,[74] a field of law in which it is necessary to analyse how digital markets actually work and that also examines a range of formal and informal legal frameworks?[75] Judges of the Court will understandably be reluctant to stray into

67 KE Klare "Legal culture and transformative constitutionalism" (1998) 14/1 *South African Journal on Human Rights* 146 at 151.

68 Id at 153.

69 C 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*" (2015) 132/4 *South African Law Journal* 711.

70 S Wilson and J Dugard "Taking poverty seriously: The South African Constitutional Court and socio-economic rights" (2011) 3 *Stellenbosch Law Review* 664.

71 S Sibanda "Not purpose made! Transformative constitutionalism, post-independence constitutionalism and the struggle to eradicate poverty" (2011) 30/3 *Stellenbosch Law Review* 482.

72 T Roux "Transformative constitutionalism and the best interpretation of the constitution: Distinction without a difference" (2005) 2 *Stellenbosch Law Review* 258.

73 See R Dworkin *Justice for Hedgehogs* (2011, Harvard University Press).

74 In our digital age, competition law will have to reckon with the intersection between market efficiency and consumer privacy. The authors' 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 Court to resolve, exercising its jurisdiction as the final arbiter of the meaning and scope of constitutional rights.

75 The doctrine of subsidiarity opens 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 case law.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

uncharted waters, especially those that threaten to erode the distinction between law and politics. However, an overanxious regard for existing boundaries will limit the court's ability to respond to the harms to constitutional democracy associated with digitalization.

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 as, before 2021, the Court had not had to engage explicitly with the implications of digitalization for privacy rights. Nonetheless, the existing body of case law will probably frame the court's 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, as well as harms that come from the increasing aggregation and dissemination of data by private companies and especially by platform companies for commercial purposes. This section examines two types of cases: those concerning the state's coercive powers of search and surveillance (comprising four cases of the Court); and those concerning constitutional control of the publication of private facts under the common law, as yet made up of cases decided by lower courts.

Search, seizure and surveillance

The first and leading Constitutional Court case in South African privacy law is *Bernstein v Bester* (*Bernstein*),[76] a "search" case in which Ackermann J provided an extended exposition of the philosophical underpinnings of the right to privacy and comparative jurisprudence. Although this case was decided under section 13 of South Africa's Interim Constitution (Interim Constitution),[77] 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 of the Companies Act 1973 that 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.[78]

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, of 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 that person's personal privacy. Regarding the determination of the scope of the right, Ackermann J adopted the "reasonable expectation" test. Under this test, there is an inviolable inner sanctum, such as family life, sexual preference and the home, which becomes progressively more attenuated as individuals enter public spaces and communal relationships with others.[79] The test has found an enduring place in the Court's privacy jurisprudence and will be important in future cases concerning the impact of digitalization on constitutional privacy.

The test is drawn from the Fourth Amendment to the US Constitution. 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*".[80] Announcing this test of an unconstitutional search, *Katz v US* significantly reversed the US Supreme

76 Above at note 42.
77 Constitution of the Republic of South Africa 1993.
78 *Bernstein v Bester*, above at note 42, para 55.
79 Id, para 67.
80 *Katz v US* 389 US 347 (1967) at 362 (emphasis added).

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

Court's earlier decision in *Olmstead v US*,[81] which had held, over an eloquent dissent by Brandeis J, that wiretapping did not amount to "trespass" as there was no physical entry and so there was no unconstitutional "search". The formulation of the new *Katz* test was an attempt to preserve 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".[82]

However, 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. 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".[83] Lessig thus asks, the authors believe appropriately, whether we need a second kind of privacy: "privacy in public".[84]

Langa J, appeared to open the door to reconsideration of the application of the reasonable expectations test in South Africa in light of technological change in *Investigating Directorate, Serious Economic Offences v Hyundai Motor Distributors*,[85] decided some years after *Bernstein*. This matter concerned the constitutionality of legislation that did not specifically require the prosecuting authorities to show reasonable suspicion as a condition precedent when applying for a judicial warrant authorizing a search. In an incidental but important dictum, Langa DP, for the Court, added the following gloss to the reasonable expectation test of the scope of constitutional privacy:

> "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."[86]

When a court reconsiders this language in a future case where the specific question before it concerns constitutional privacy in the time of digitalization, it will have to consider when and whether individuals are able to decide effectively what information to reveal publicly. Much of the collecting, permanent recording and transfer of data today occurs 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, as will the nature of the constitutional enquiry into both subjective and objective reasonableness.

The relevant case subsequent to *Bernstein* was also a physical search case under the Interim Constitution. In *Mistry v Interim National Medical and Dental Council* (*Mistry*),[87] legislative powers 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

81 277 US 438 (1928).
82 L Lessig *Fidelity and Constraint: How the Supreme Court Has Read the American Constitution* (2019, Oxford University Press) at 264.
83 Lessig *Code: 2.0*, above at note 12 at 203.
84 Id at 202.
85 2001 (1) SA 545 (CC).
86 Id, para 16 (emphasis added).
87 Above at note 59.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

files that might contain a person's last will and testament, private letters and business papers".[88] In finding that the statutory authority to enter private homes without a warrant and 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.[89] While leaving open other textual sources, including the right of access to information, the Court effectively recognized 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".[90] *Mistry* went on to say that whether this privacy right is violated depends on the intrusiveness of the manner in which the information is obtained, whether it is about intimate aspects of personal life, whether it involves data provided for one purpose that was then used for another and 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.[91]

Although the matter did not examine the implications of digitalization for data collection, processing and dissemination, the influence on *Mistry* of a case of the German Constitutional Court,[92] the case that first recognized a personal right to control private information, is clear. In this 1983 case, the German Constitutional Court engaged the digitalization question directly: "[t]he 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 behaviour because of the psychological pressure that public awareness may place upon the individual".[93]

The fourth case is *AmaBhungane v Minister of Justice and Correctional Services*,[94] which concerned the constitutionality of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002 (RICA) under the general right of constitutional privacy in section 14 of the Constitution, despite the fact that the section also specifically prohibits "searches of one's person and home"[95] and protects the privacy of communications.[96] A 2021 decision, it is the most recent and most important case in this context, because the 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

In the Court's telling, the adoption of RICA was "informed by considerable technological developments in electronic communications",[97] as the legislation authorizes "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".[98] 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"

88 Id, para 21.
89 Id, para 23.
90 Id, para 48.
91 Id, para 51.
92 *The Census Act Case* (1983) 65 (B VerFGE 1).
93 See DP Kommers and RA Miller *The Constitutional Jurisprudence of the Federal Republic of Germany* (3rd ed, 2012, Duke University Press) at 409 and 411.
94 Above at note 6.
95 RICA, sec 14(a).
96 Id, sec 14(d).
97 *AmaBhungane v Minister of Justice*, above at note 6, para 7.
98 Ibid.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

into its lexicon and analysis. This includes searches by technology. The opening paragraph of the judgment states:

> "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 weaponised 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.*"[99]

The first point to be made about the Court's rights analysis in terms of the constitutional right to privacy is that it attached particular importance to constitutional privacy in the light of South Africa's experience under a "police state".[100] It said the privacy right is "axiomatically … singularly important in South Africa's constitutional democracy".[101] The Court added that invasion of an individual's privacy rights infringes the "cognate right to dignity",[102] which the Court has termed elsewhere the "cornerstone of South African democracy".[103] The effect of this reasoning is to strengthen privacy protection and to require persuasive justification for state action that invades the right.

It is a short step from here to recognize the particular threats posed by digital policing to constitutional privacy, which are evident in the paragraph quoted above. Yet the Court also continues to rely on the *Bernstein* privacy paradigm, which affords strong protection for intimacy but works less well as a framework for identifying the threats posed by digital policing to constitutional privacy. The Court reasoned as follows: "[i]magine 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".[104] 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".[105] However, is surveillance and monitoring, with our knowledge, of communications that are not intimate less disturbing and invasive? The Court appears to recognize potential problems with its reasoning, which arise from the impact of digitalization on the boundary between the private and the public or, as Lessig would term it, "privacy in public".[106] It acknowledges that the legislation "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".[107]

After finding that there can be no question that "surveillance of private communications limits the right to privacy",[108] the Court then considered whether the limitation is "reasonable and

99 Id, para 1 (emphasis added).
100 Id, para 26.
101 Id, para 27.
102 Id, para 28.
103 *National Coalition for Gay and Lesbian Equality and Others v Minister of Home Affairs and Others* 2000 (2) SA 1 (CC), para 28.
104 *AmaBhungane v Minister of Justice*, above at note 6, para 23.
105 Id, paras 23–24.
106 Lessig *Code: 2.0*, above at note 12 at 202.
107 *AmaBhungane v Minister of Justice*, above at note 6, para 25 (emphasis added).
108 Ibid.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

justifiable in an open and democratic society based on human dignity, equality and freedom".[109] 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 that the basic structural elements of RICA are unconstitutional. In essence it said that RICA did not pass the test of constitutionality because its design features fell short of what the rule of law requires, in that it failed to provide safeguards for independent judicial supervision and for the notification of subjects of surveillance; it allowed the police to seek permission to intercept on an ex parte application without adequate safeguards; 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.[110] 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".[111] 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.

Of these four cases, only the 2021 matter, *AmaBhungane*, engages with the consequences of digitalization. On a superficial reading, the earlier cases of *Bernstein, Hyundai Motor Distributors* and *Mistry* would not appear to offer much to those concerned with the dangers posed to privacy by digitalization. However, a reading of them based on dignity rather than narrowly on liberty has emphasized the links and the potential these types of cases have in safeguarding the concept of privacy in public and the right of information privacy. However, 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.

Publication, dissemination and use

Before the adoption of the Constitution and the right to privacy, and before the Interim Constitution was introduced, the South African legal system recognized the right to privacy as an independent personal right under the common law of delict, the *actio iniuriarum*. 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*[112] the Appellate Division, the country's highest court at the time, clarified that a breach of privacy under 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 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.[113] It has been suggested that the latter is more properly considered as a breach of the separate right to an identity.[114] However, in *Bernstein*, Justice Ackermann pointed to the close relationship between privacy and "what is necessary to have one's own autonomous identity".[115] In agreement with McQuoid-Mason, the post-1994 Supreme Court of Appeal extended protection to features of a person's identity in *Grutter v Lombard*[116] under the *actio iniuriarum*. Appropriation of an individual's image or likeness for the benefit of another, or for commercial

109 Ibid.
110 Id, para 157.
111 Id, para 129.
112 1993 (S) SA 451 (AD).
113 D McQuoid-Mason "Invasion of privacy: Common law v constitutional delict" (2000) *Acta Juridica* 227.
114 J Neethling, JM Potgieter and PJ Visser *Law of Delict* (4th ed, 2001, Butterworths) at 284.
115 *Bernstein v Bester*, above at note 42, para 65.
116 2007 (4) SA 89 (SCA).

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

purposes and without consent, therefore constitutes an actionable breach of privacy rights under both South African common law and the Constitution,[117] on which further below.

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) recognized under common law to provide protection against the specific harms associated with digitalization. As noted above, digitalization 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.[118] While the detail must await further research, we can offer a high-level answer here to the question of what relief the law of delict provides. The answer is some protection, but that the conceptual structure of the law of delict as designed to remedy specific, discreet and quantifiable harms does not reach the systemic issue of power or Solove's aggregation problem.[119] The delicts are all furthermore currently cast in the paradigm of concealment and secrecy.[120] The delict of intrusion, for instance, can provide only limited protection in the face of the consolidation of public records in centralized databases, and the collection and dissemination of information in cyberspace, which is a public space. Of course, we do not yet know how the Court will use its powers to develop the common law in response to digitalization and we do not yet know whether it will recognize a new "constitutional delict" for the breach of privacy rights as proposed by McQuoid-Mason. The authors' 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 Emile Zitzke, reflecting on the award for damages for 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.[121]

The two delicts with the greatest potential, in the authors' 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 facts delict has thus far primarily been invoked against traditional mass media. But who are the media today? And what constitutes "publication" in the time of digitalization? 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 law.[122]

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. However, under South African law, it is not clear whether they can attract liability as other media companies do 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 2002 immunizes internet service providers that are "mere conduits" from liability for "providing access to, or for operating facilities for information

117 Id, para 9.

118 Ben-Shahar "Data pollution", above at note 17. These "data emissions", which are increasingly leaked into the digital ecosystem, are harmful to private and individual interests, and 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. However, the authors see no reason why an individual who has suffered demonstrable harm should not be able to recover damages under common law or under a newly minted "constitutional delict".

119 DJ Solove "Privacy and power: Computer bases and metaphors for information privacy" (2001) 154 *Stanford Law Review* 1393.

120 Id at 1439.

121 E Zitzke "The Life Esidimeni arbitration: Towards transformative constitutional damages?" (2020) 3 *Journal of South African Law* 419.

122 J Balkin "Information fiduciaries and the First Amendment" (2016) 49/4 *UC Davis Law Review* 1183.

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press

systems, or for information systems or transmitting, routing or storage of data messages". So far as the authors are aware, there is as yet no South African case in which monopolistic platform companies or other web-based publishers have been sued under common law. However, individuals who post material are treated as publishers and can be held liable under common law. This is what happened in a recent case, *Economic Freedom Fighters and Others v Trevor Manuel*,[123] in which a former minister successfully sued members of a political party under common law for delictual damages for posting defamatory statements about him on Twitter. The corporation owning the digital platform was not cited as a respondent. However, what about other kinds of harms to privacy that result from digital processing of personal information or result from the 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, to what constitutional standards can and should they be held? These questions have not yet been answered. However, the authors think that within our system of constitutional democracy exist considerable normative and institutional resources to develop a "public law paradigm" that is responsive to the risks to privacy and other rights in our age of digitalization.

Conclusion

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

First, the article argued that this question is best answered through the lens of a South African public law perspective. In the authors' 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 digitalization.

Secondly, it argued that the South African constitutional text instantiates a rights-orientated and rule-of-law-centred political theory that potentially facilitates the development of a privacy law adequate for the digital age. This view takes into account South Africa's transformative Constitution, with particular characteristics, including the components of horizontality and subsidiarity.

The 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 cases addressing surveillance harms and those resolving disputes addressing the harms associated with publication, dissemination and use. The article argued 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 the potential to do so. The authors acknowledged the creative potential of proportionality / rule-of-law analyses simultaneously to focus on the need for systemic controls of harms to privacy and democracy, and to recognize the need to incorporate an assessment of the benefits for sectors such as law enforcement and social rights in the constitutional analysis.

Delving into and drawing from one particular national context, in developing our public law perspective, this article has 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 digitalization.

Competing interests. None

123 2021 (3) SA 425 (SCA).

Cite this article: Cachalia F, Klaaren J (2024). Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization. *Journal of African Law* **68**, 89–107. https://doi.org/10.1017/S0021855323000268

https://doi.org/10.1017/S0021855323000268 Published online by Cambridge University Press