Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Privacy boundaries in digital space: an exercise in responsibilisation

Mo Egan

To cite this article: Mo Egan (2022): Privacy boundaries in digital space: an exercise in responsibilisation, Information & Communications Technology Law, DOI: 10.1080/13600834.2022.2097046

To link to this article: https://doi.org/10.1080/13600834.2022.2097046

Published online: 05 Jul 2022.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
https://doi.org/10.1080/13600834.2022.2097046

Routledge
Taylor & Francis Group

Privacy boundaries in digital space: an exercise in responsibilisation

Mo Egan

Division of Law and Philosophy, Faculty of Arts & Humanities, University of Stirling, Stirling, United Kingdom

ABSTRACT

In digital space, the boundaries of privacy are often amorphous, symptomatic of human actors' developing relationship with virtual spaces. As a result, those with little exposure to digital space may simply transplant their 'real world' expectations, whereas those who immerse themselves may assimilate a new perspective on privacy. Firstly, this paper considers the need for comparative research in the privacy field. Secondly, it reflects on the utility of Altman's and Hughes' theories of privacy regulation in the context of digital space. Thirdly, it discusses how privacy interference has been addressed by UK and South African law, focusing on the evolution of data protection. Fourthly, it reflects on the legal implications of the fracturing of responsibility between state and non-state actors. And, lastly, it draws out the consequences of such responsibilisation and how these relate to Altman and Hughes' work.

KEYWORDS

Privacy; data protection; culture

1. Introduction

Digital space is invigorating. There are opportunities to express oneself in new, creative, and innovative ways. There are opportunities to re-invent oneself. Both an individually created persona, and technical innovations, introduce characters into the ecology of the internet that can impact on the privacy rights of others. Understanding this evolution of digital society is critical to the legal regulation of digital technologies. Without such understanding there is a risk that regulation will not be fit for purpose. It may do more harm than good. Bad regulation can have a detrimental impact on public trust and public trust is critical to compliance.[1] However, the regulation of privacy presents a challenge because of the tension between an individualistic interpretation of privacy rights and the public interest in the operation of privacy boundaries.[2]

For example, the individual right to privacy can (generally speaking) be outweighed in circumstances where there is suspicion of criminality. This is specifically recognised in the

CONTACT Mo Egan mo.egan@stir.ac.uk

[1]Tom R Tyler, 'Public Trust and Confidence in Legal Authorities: What do Majority and Minority Group Members Want from the Law and Legal Institutions?' (2001) 19 Behav Sci Law 215–235, 232.

[2]Mark O'Brien, 'Law, privacy and information technology: a sleepwalk through the surveillance society?' (2008) 16(1) Information & Communications Technology Law 25–35, 34.

limitations on the right to privacy set out in Article 8 of the European Convention of Human Rights. Yet, in the last ten years or so, there has gradually been greater recognition of the relationship between individual private rights and the public interest in the protection of those individual rights.[3] This is particularly so in the case of digital space where individuals have become dehumanised into data.[4]

Data is commercial gold. The potential for commercial exploitation was in large part responsible for a shift towards acknowledging that there is a collective public good in the protection of (personal) data and a re-consideration of how this aspect of privacy can be protected. Still, the boundaries of privacy in digital space, as with the rest of its architecture, have shifted in the face of technical capability and the relationship that is fostered between that technical capability and its masters.[5] While those initial masters are often commercial innovators, new masters are entering the fray as the responsibility to protect privacy is dispersed.

Since the breadth of conduct that could be considered to raise privacy concerns is extremely broad, it is necessary to focus on specific examples that provide insights into how privacy boundaries are prospectively being defined through (formal and informal) regulation. Here, the focus will be on data protection where the UK and South Africa can offer useful comparative insights into the regulation of privacy boundaries because there has been a recent focus on the regulation of behaviour in digital space.

Firstly, this paper considers the need for comparative research in the privacy field. Secondly, it considers the utility of Altman's and Hughes' theories of privacy regulation in the context of digital space. Thirdly, it discusses how privacy interference has been addressed by UK and South African law, focusing on the evolution of data protection. Fourthly, it reflects on the legal implications of the fracturing of responsibility between state and non-state actors. And, lastly, it draws out the consequences of such responsibilisation and how these relate to Altman and Hughes' work.

2. Decolonising privacy

When examining an issue such as the scope of a right to privacy it is very easy to become entrenched in a parochial view of a primary (Western) jurisdiction.[6] This becomes even more entrenched when there is evidence that aspects of regulation have become a global phenomenon. For example, the EUs General Data Protection Regulation is frequently held out to be one such regulatory success story, influencing the protection of personal data across the globe.[7] Or, when communities of scholarship become so dominant that they reify one another's perspective.[8] However, scholars should be wary of the assumption that another jurisdiction adopts a similar system and equally, even where it does so, consideration should be given to the operationalisation of that system since the law on the books may differ from that in action.

[3]See for example, *Lloyd v Google LLC* 2019 WL04804855.
[4]Carissa Veliz, *Privacy is Power: Why and How You Should Take Back Control of Your Data*, (Bantam Press, 2020) at p. 1.
[5]Lawrence Lessig, 'Cyberspace and Privacy: A New Legal Paradigm: Foreword' (2000) 52 Stan L Rev 987, 990.
[6]Payal Arora, Decolonizing Privacy Studies, (2019) 20(4) Television & New Media, 366–378, 368. DOI: https://doi.org/10.1177/1527476418806092.
[7]Elif Kiesow Cortez (ed), *Data Protection Around the World: Privacy Laws in Action* (Asser Press, 2020), p. 6.
[8]For example, much privacy scholarship begins discussion citing S. D. Warren and L.D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard law Review 193. See also, S. Gutwirth, *Privacy and the Information Age* (Rowman and Littlefield, 2002) at p. 1.

Still, there also needs to be caution in the presumption of difference.[9] In the context of digital space, there is a problem where similarities and differences are not understood. The problem is the potential for conflict between the approach of one jurisdiction and another in developing regulations. And, in turn, what that means for an individual who is seeking to protect their privacy. It is argued here that central to resolving such conflicts will be developing an understanding of privacy as it manifests in a diverse range of jurisdictions. Comparative research is essential.[10] This paper will make a contribution to this dialogue by examining the position of the UK (a global north country) and South Africa (a global south country). Significantly, in the UK, the Government have introduced their Online Safety Bill, the Law Commission has recently published their report on modernising communications offences, and they have issued their consultation paper on intimate image abuse.[11] And, in South Africa, the final provisions of the Protection of Personal Information Act 2013 have been brought into force and the Cybercrimes Act 2020 has been passed.[12]

Importantly, the entanglement of the UK and South Africa's colonial history, South Africa's journey to independence and its constitutional restructuring offer a rich tapestry within which to explore the development of privacy and its protection. Moreover, since these jurisdictions have recently attempted to implement the regulation of digital space, they offer valuable contemporary perspectives on where privacy boundaries are set.

3. Achieving equilibrium in privacy boundaries

There are three aspects to be considered in defining privacy boundaries in digital space. There is a need to examine boundaries that are established by existing legal regulation, there are those boundaries that have not yet been, but should be, recognised through legal regulation, and there are those that are practically implemented, either through technical means (such as security software) or human action (for example, electing not to accept cookies). Those that are practically implemented are critical because they effectively determine an individuals' level of privacy – regardless of the scope of the legal right. As Neethling has argued 'the concept of privacy cannot be determined by legal principles, but primarily by its nature in the sphere of factual reality'.[13] Indeed, the reality of privacy boundaries is that their legally recognised scope will only partially reflect the expectation and whether that expectation can ever be delivered through the creation and enforcement of legal regulation is debateable. While a jurisprudential definition and delineation of privacy can rightly be recognised as 'essential to enable protective measures to be properly applied in practice' a disconnection between expectations and legal protection can lead to a lack of legitimacy in that system of regulation.[14]

[9]Alex B. Makulilo, ' "A Person Is a Person through Other Persons"—A Critical Analysis of Privacy and Culture in Africa' (2016) 7 Beijing Law Review 192–204. DOI: https://doi.org/10.4236/blr.2016.73020.
[10]L. Bygraves, 'Privacy Protection in a Global Context – A Comparative Overview' (2004) Scandinavian Studies in Law, 47, 319–348.
[11]Online Safety Bill 2021; Law Commission, Modernisation of Communication Offences, Final Report, Law Com No 399, July 2021. Available: https://www.lawcom.gov.uk/project/reform-of-the-communications-offences/ Accessed 11 August 2021; Law Commission, Intimate Image Abuse: A Consultation Paper, No 253. February 2021.
[12]Protection of Personal Information Act No 4 of 2013. Commencement date 1 July 2020. Cybercrimes Act 2020.
[13]J Neethling, 'The Concept of Privacy in South African Law' (2005) 122 S African LJ 18, 19.
[14]ibid.

Still, the need to reflect on current approaches to defining and operationalising privacy boundaries is important. With the rise of COVID-19 and as the pandemic has ravaged country after country, the ways in which privacy boundaries are established in digital society are renewed, reinvigorated, and recast. The relationship between the state and the individual has been challenged as countries introduce methods of tracking and tracing their population for the purposes of public health protection.[15] Moreover, the relationship between individuals has been challenged as quarantine restrictions shift real world interactions online and create new opportunities for digital invasion of privacy.[16]

Despite vocal opposition to interference with privacy boundaries, many scholars have highlighted that individuals' actions reveal little meaningful effort to protect those boundaries. People 'routinely give out their personal information and willingly revealing intimate details about their lives on the internet'.[17] Indeed, Austin argues that '[i]f we want to exploit the opportunities offered by a networked world, as the growing popularity of the internet indicates that we do, then privacy seems to be the price'. [18] Still, this author takes issue with such claims. There are critical questions to be asked about the extent to which individuals understand the implications of their actions and indeed whether they are consenting to the ways in which such information can be utilised. To answer such questions, it is necessary to consider how privacy boundaries are set.

4. Behavioural mechanisms as boundary setting

Altman makes a strong case for the recognition of the multifarious ways that behavioural mechanisms offer insight into how individuals protect their privacy in practical terms. He argues that privacy is achieved through an 'interpersonal boundary process by which a person or group regulate interactions with others'.[19] Significantly, his view is that it is a 'dynamic process involving selective control over a self-boundary'.[20] However, while placing the individual at the centre of this quest to marry desired privacy and achieved privacy, Altman acknowledges that different cultures have developed different behavioural mechanisms for 'managing the social accessibility of people to one another'.[21]

Certainly, this can be seen in the South African foundation value of Ubuntu. Ubuntu has been described as 'a community-based mindset in which the welfare of the group is greater than the welfare of a single individual in the group'.[22] Significantly, Olingera et al. contend that while 'individualistic cultures of the West argue that personal

[15]Kim Barker; Uribe-Jongbloed, Enrique and Scholz, Tobias, 'Privacy as Public Good – A Comparative Assessment of the Challenge for CoronApps in Latin America' (2020) 1(1) Journal of Law, Technology & Trust, 1–24. DOI: https://doi.org/10.19164/jltt.v1i1.1006.

[16]K. Bracewell; P. Hargreaves and N. Stanley. 'The Consequences of the COVID-19 Lockdown on Stalking Victimisation' (2020) Journal of Family Violence DOI: https://doi.org/10.1007/s10896-020-00201-0.

[17]Daniel Solove, *Understanding Privacy* (Harvard University Press, 2009) at p. 5.

[18]Lisa Austin, 'Privacy and the Question of Technology' (2002) 22(2) Law and Philosophy 119–166. Available: https://www.jstor.org/stable/3505151.

[19]Irwin Altman, *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding.* (Brooks/Cole Publishing, 1975) at p. 6.

[20]ibid.

[21]ibid 12.

[22]Hanno N. Olingera, Johannes J. Britza, b and Martin S. Olivier, 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa', (2007) 39(1) The International Information & Library Review, 31–43, 33. DOI: https://doi.org/10.1080/10572317.2007.10762729.

privacy is required for a person to express his true individuality', within Ubuntu 'individuality is discovered and expressed together with other people and not alone in some autonomous space'.[23] As a consequence, Olingera et al. argue that personal privacy plays no role in this Ubuntu context.[24] However, in making these observations, Olingera et al. were focused on the 'legal protection' of privacy and so were not addressing specifically the behavioural privacy protection that may still play a role in Ubuntu culture. The fact that a lower value is attached to individual privacy in the face of group interests does not automatically negate recognition of the individual right. Still, if Altman's theory of privacy is to be taken seriously, privacy regulation may be secured differently in the Ubuntu context. However, it has been suggested that the dominance of Ubuntu is waning as African communities become more exposed to Western influences and as technologies advance.[25] As a consequence, there is a need for empirical research to explore the evolution of the right to privacy as the 4th industrial revolution is pursued.[26]

Although focused on interpersonal interaction in the physical world, Altman's analysis has much to offer the development of privacy regulation in digital space. Altman identifies four behavioural mechanisms that can be used to regulate privacy: verbal, non-verbal, environmental, and culturally based mechanisms.[27] Firstly, Altman's verbal mechanisms refer to the content and structure of verbal communication. For example, shouting 'keep out' to your teenage son. He argues that this verbal communication is the 'main vehicle of social interaction'.[28] However, while it is possible to record and transmit verbal communications through the internet, it may be more appropriate to expand this mechanism to a verbal or textual mechanism. This would accommodate that within digital space much communication is facilitated via the communication of text.[29] Secondly, Altman's 'non-verbal' mechanisms identifies the role of body language in the communication of privacy boundaries. Although, this may not be pervasive in digital space, it can, of course, continue to play a role where a visual medium is adopted, such as the use of video-calling or conferencing software or through use of an avatar. Thirdly, Altman's 'environmental' mechanism broadly encompasses the clothes an individual chooses to wear, the assertion (or not) of personal space, and territorial behaviour. This too can be translated into the digital world since an individual can choose, for example, to post profile pictures, create avatars, and establish their own territories through the creation of individualised digital spaces, such as Facebook profiles or Instagram accounts. Fourthly, Altman's 'culturally based' mechanisms recognises that specific cultures adopt different privacy management strategies. However, in the context of digital space, there can be a tendency to consider it as one homogeneous social space and by extrapolation, approaches to the control of behaviour can lack sensitivity to cultural nuances. Since privacy can be influenced by culturally embedded

[23]ibid 36.
[24]ibid.
[25]Makulilo (n9)194.
[26]Noting that this is likely to be a turbulent process, as discussed in Ewan Sutherland 'The Fourth Industrial Revolution – The Case of South Africa'(2020) 47(2) Politikon 233–252, DOI: https://doi.org/10.1080/02589346.2019.1696003.
[27]Altman (n19) 32–42.
[28]ibid.
[29]Kim, Barker and Olga, Jurasz, 'Text-Based (Sexual) Abuse and Online Violence Against Women: Toward Law Reform.' In: Bailey, Jane; Flynn, Asher and Henry, Nicola eds. *The Emerald International Handbook of Technology Facilitated Violence and Abuse. Emerald Studies In Digital Crime, Technology and Social Harms.* (Bingley: Emerald Publishing Limited, 2021) pp. 247–264. DOI: https://doi.org/10.1108/978-1-83982-848-520211017.

practices, so cultures can collide as they attempt to navigate 'interpersonal boundary process' in this digital landscape.[30] Collectively, Altman's four behavioural mechanisms allow the individual to achieve their desired level of privacy controlling the boundary between the self and others guided by embedded cultural norms.

5. Legal recognition of boundary setting

While Altman's construction of the way individuals choose to 'regulate' their privacy is important, there remain questions as to when privacy can and should be provided specific legal protection and to what extent this protection should reflect the exercise of such behavioural mechanisms as noted above.[31]

Hughes has proposed that 'if we accept that an individual has taken steps to obtain or maintain privacy, steps which should be respected, then we reduce the need to develop an over-broad system of regulation through the codification of normative rules'.[32] In turn, she argues by respecting such boundaries, individuals are given 'greater scope to achieve the level of privacy which they desire'.[33] This is able to happen because 'they are not restricted to the objective forms of privacy prescribed by judicial and societal perceptions of privacy'.[34]

This is an interesting proposal since it suggests that we should not look to the law to provide regulation of privacy boundaries. Hughes appears to suggest that a behavioural theory of the right to privacy would determine that the principal normative rule would be that where steps have been taken to obtain or maintain privacy, that privacy should be respected. Where that rule fails, there may be circumstances where alternative normative rules are codified through legal protections. However, this argument falters because asserting that *inaction* is acceptance of a privacy incursion would go too far.

There is a difference between not knowing that you need privacy barriers in place to signal your desire to protect your privacy and expressly choosing not to erect those barriers in light of that knowledge. In addition, there may be circumstances where an individual's constitution is such that they are not in a position to make those choices, with Hughes providing the example of children.[35] Certainly, this position appears to be reflected in South Africa's approach to the protection of personal information. It prohibits the processing of children's personal information unless an exception applies or responsible parties have requested authorisation.[36] Similarly, the UKs approach also provides heightened protection to children[37] having recently enhanced measures specifically seeking to support the participation of children in the information society.

In particular, the UKs Age Appropriate Design Code set out to ensure that children are protected in their engagement with online services.[38] Having come into force on the 2

[30]Altman (n19) 6.
[31]Stephen T. Margulis, 'On the Status and Contribution of Westin's and Altman's Theories of Privacy' (2003) 59(2) Journal of Social Issues, 411–429.
[32]Kirsty Hughes, 'A behavioural understanding of privacy and its implications for privacy law' (2012) 75(5) MLR 806–836, 815.
[33]ibid.
[34]ibid.
[35]Hughes (n32) 820.
[36]s34–35, Protection of Personal Information Act No 4 of 2013.
[37]s18 Data Protection Act 2018. c12.
[38]ICO, Age Appropriate Design Code, 2 September 2020.

September 2020 and allowing for a one year transition period, it can be anticipated that we will see a flurry of changes as organisations attempt to comply.[39] Of particular importance, it emphasises the need for a tailored approach to privacy in respect of children. Accordingly, it requires that in the context of online products and services 'settings must be "high privacy" by default (unless there's a compelling reason not to); only the minimum amount of personal data should be collected and retained; children's data should not usually be shared [and] geolocation services should be switched off by default. Nudge techniques should not be used to encourage children to provide unnecessary personal data, weaken or turn off their privacy settings'.[40] Significantly, it has extraterritorial effect as it applies to both those based in the UK and those who provide products and services that can be accessed by children in the UK.[41] In this way, new masters are responsibilised such that a failure to comply with the code has enforcement implications. If these online services 'fail to conform to a provision of this code [they] may find it difficult to demonstrate compliance with the law and [they] may invite regulatory action'.[42]

However, in relation to the general population, Hughes indicates that in the first instance, the obligation is on the individual to take steps to erect physical or behavioural barriers and that in doing so other individuals should be aware of those barriers and respect them. The role of law then is to provide a remedy where an individual's barriers have been breached.

Hughes goes so far as to emphasise the individual's obligation to erect *sufficient* privacy barriers. She argues that such barriers should be taken into account when considering whether there is a privacy violation. However, she does suggest that since privacy is mutually created the intention of the person carrying out the suggested privacy invasion may also be taken into account in establishing whether a violation has taken place.[43] She does concede that this does not help to determine when the law should provide a remedy for such a violation but that an individual's intentions may influence when their conduct was justified and, therefore whether the law should provide a remedy.

This is an interesting observation and appears, in part, to reflect the approach taken in SA. The data protection framework provides that the data subject can issue civil proceedings against a responsible party, or, the regulator prompted by a data subject and that action can be pursued regardless of the intention or negligence of the responsible party.[44] However, it is notable that in defence the responsible party can rely on the '*fault* [author's emphasis] on the part of the plaintiff'.[45] This defence demonstrates the responsibilisation of individuals for their own privacy preservation.

6. Recognition of public and private (privacy) harms in the UK and South Africa

Altman and Hughes make clear that the boundaries of privacy are established by the exercise of behaviour mechanisms. For Altman, through the verbal, non-verbal,

[39]Laid before Parliament by the Secretary of State under s125(1)(b) Data Protection Act 2018 on 11 June 2020.
[40]ICO, Age Appropriate Design Code, 2 September 2020. At p. 4.
[41]ICO, Age Appropriate Design Code, 2 September 2020. At p. 9.
[42]ICO, Age Appropriate Design Code, 2 September 2020. At p. 9.
[43]Hughes (n32) 820.
[44]s99(1) Protection of Personal Information Act No 4 of 2013.
[45]s99(2)(b)–(d) Protection of Personal Information Act No 4 of 2013.

environmental, and cultural manifestations. For Hughes, these boundaries can be self-regulated through the exercise of mutual respect. However, she also acknowledges specific circumstances where the law may have to step in. Those circumstances include, where there is a threat to privacy that may have a 'chilling effect' on social interaction, where a privacy violation prevents another from enjoying their own privacy, or where there is a cumulative effect of minor erosions of privacy.[46] Still, in order for mutual respect to become embedded both parties would have to attach the same value to privacy. However, the value attaching to privacy in digital space appears to fluctuate. Part of that fluctuation is, in this author's view, influenced by an individual's understanding of what privacy is being sacrificed and to whom. Without that understanding, there is no conscious boundary setting that Altman and Hughes advocate. For this reason, in order for legal regulation of this space to be legitimate it must find a balance in the facilitation of self-regulation and the setting of legal rules that can protect those who are not in a position to anticipate privacy intrusions.

6.1. Infrastructure and engagement

In South Africa, the development of digital infrastructure continues to present challenges with lower level of penetration and usage of the internet.[47] The wider indication of Africa's development as an information society, is that it 'lags behind the rest of the world'.[48] However, it is not only the availability of ICT that creates a problem but that social, economic, and cultural dynamics influence whether or not there is engagement with the available ICT.[49] There is some evidence to suggest that younger people have high levels of access but continue to lack a sense of cyber safety.[50] This is important because it is through that engagement that the 'traditional' interpretations of privacy boundaries are challenged. As digital society evolves, so too will expectations that legal protection encompasses the digital person as an extension of self. Indeed, as highlighted by Hughes, where individuals are not aware that they can/should adopt practical or technical privacy barriers, the law should evolve to provide some protection to those more vulnerable individuals.

In the UK, by the end of 2020, 94% of UK homes had internet access.[51] However, 18% of those over 65 and 11% of those in a lower socio-economic household did not have access.[52] This creates what has been termed a 'digital divide' meaning that certain groups are disproportionately impacted by this exclusion from digital society.[53] While in 2018, it was reported that 62% of South African households had internet access, this

[46]Hughes (n32) 816–819.
[47]National Development Plan 2030, Chapter 4 Economic Infrastructure; Genna Robb and Ryan Hawthorne, 'Net Neutrality and Market Power: The Case of South Africa', 29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a Digital Future: Turning Technology into Markets?", Trento, Italy, 1st–4th August, 2018, International Telecommunications Society (ITS), Calgary. Available at: http://hdl.handle.net/10419/184964 at p. 1.
[48]Elirea Bornman, 'Information society and digital divide in South Africa: results of longitudinal surveys' (2016) 19(2) Information, Communication & Society, 264–278, 265. DOI: https://doi,org/10.1080/1369118X.2015.1065285.
[49]ibid 267.
[50]Elmarie Kritzinger, 'Cultivating a cyber-safety culture among school learners in South Africa' (2017) 14(1) Africa Education Review, 22–41, 22. DOI: https://doi,org/10.1080/18146627.2016.1224561.
[51]Ofcom, Online Nation Report 2021. Available at: https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/online-nation Accessed 25 March 2021. At p. 3.
[52]ibid.
[53]ibid.

included access from work and mobile services as well. In 2021 it was reported that this had increased slightly to 64%.[54] However, the digital divide is also present in the South African context, with a distinction drawn between the rural and urban experience. This distinction is caused by a lack of basic ICT infrastructure and electricity to rural communities.[55] In addition, while the expense of purchasing digital devices is prohibitive for some, the cost of data is a greater inhibitor of access to the internet.[56]

By the age of 15, Ofcom reports that in the UK, 95% of children engaged with social media and 59% did so by the age of 11.[57] This means that that 59% were using the service in violation of terms of service, which in most platforms is set at the age of 13.[58] Ofcom also indicates that 'unwelcome friend requests/follows and trolling were the most common potentially harmful types of contact across all platforms'.[59] A small scale South African study reported that 70.4% of participants aged between 7 and 19 used the internet in 2016 and 86.3% had a social networking account.[60] It is difficult to identify robust data on the prevalence of online harms in general, and within specific demographics, experienced in South Africa. In turn, this makes it difficult to address concerns that research 'disproportionately draws from empirical evidence on privacy attitudes and behaviours of Western-based, white, and middle-class demographics to theorise privacy in this digitally mediated world'.[61] That being said, concerns as to the potential of online harm escalating (to include threats to personal data) is apparent in South Africa in the passage of both the POPI Act and the Cybercrimes Act 2020.[62]

In digital space the boundaries of privacy are often amorphous, symptomatic of human actors' developing relationship with virtual spaces. Importantly, the digital infrastructure of a nation will have a significant impact on the accessibility of digital technologies and their influence on society. As a result, those with little exposure to digital space may simply transplant their 'real world' expectations whereas those who immerse themselves may assimilate a new perspective on privacy. These expectations will have an impact on the construction of harms and the adoption of behavioural mechanisms to prevent those harms. In turn, it may be necessary for legal regulation to establish alternative mechanisms that distributes the responsibility for policing those harms.

[54]Datareportal, Digital 2021: South Africa Report. Available at https://datareportal.com/reports/digital-2021-south-africa Last accessed 26 August 2021.

[55]A.I. Ilorah, and others, 'Issues and challenges of implementing mobile e-healthcare systems in South Africa' (2017) 20(3) African Journal of Biomedical Research, 249–255 cited in Mphahlele, M.I., Mokwena, S.N. & Ilorah, A., 'The impact of digital divide for first-year students in adoption of social media for learning in South Africa' (2021) 23(1) South African Journal of Information Management, a1344, 2. DOI: https://doi.org/10.4102/sajim.v23i1.1344.

[56]A. Gillwald,, O. Mothobi, & B. Rademan, 'The state of ICT in South Africa' (2018) researchICTafrica.net, viewed 25 October 2020, from https://researchictafrica. net/after-access-south-africa-state-of-ict-2017-south-africa-report_04/ Cited in Mphahlele, M.I., Mokwena, S.N. & Ilorah, A., 'The impact of digital divide for first-year students in adoption of social media for learning in South Africa' (2021) 23(1) South African Journal of Information Management, a1344, 2. DOI: https://doi.org/10.4102/sajim.v23i1.1344.

[57]Ofcom (n51) 5.

[58]ibid.

[59]ibid 6.

[60]Joanne Phyfer, Patrick Burton, and Lezanne Leoschut, 'Global Kids Online South Africa: barriers, opportunities and risks. A glimpse into South African children's internet use and online activities.' Global Kids Online, Jossel, Liesa (ed.) Centre for Justice and Crime Prevention, Cape Town, South Africa (2016) ISBN 9780620728430. At p. 8.

[61]Arora (n6) 368.

[62]Justice and Correctional Services, Cybersecurity and Cybercrime Bill: briefing, with Deputy Minister, 30 May 2017. Parliamentary Monitoring Group website**:** https://pmg.org.za/committee-meeting/24496/ Accessed 27 August 2021.

6.2. Approaches to the regulation of privacy

A comparative analysis of privacy boundaries is valuable because it tests Altman and Hughes' hypothesis that privacy is culturally embedded, as well as challenging dominant Western privacy narratives.[63] The UK and South Africa are particularly important because, as examples of global north and global south approaches, it offers the opportunity to consider the implications of political stability, technological infrastructure, and established systems of regulation in the ability to meaningly defend privacy boundaries in digital space. It is also important to consider the implications of the South African experience of developing privacy boundaries in light of its colonial/postcolonial influences.[64]

The political history of the Apartheid state plays a significant part in the need for and construction of the constitutional protection of privacy in South Africa. This has been continually reaffirmed in the jurisprudence of the constitutional court. For example, in a case involving consideration of the legality of search and seizure, Judge Sachs has explained that

> generations of systematised and egregious violations of personal privacy [had resulted in] established norms of disrespect for citizens that seeped generally into the public administration and promoted amongst a great many officials' habits and practices inconsistent with the standards of conduct now required.[65]

Similarly, in another case involving warrantless searches, Judge Madlanga highlighted that 'to the apartheid state the oppressed majority had no privacy to be protected; and no dignity to be respected … Most certainly for effect and possibly heightened indignity, many of the egregious searches were conducted at the dead of night'.[66] He acknowledged that as a result, 'the sense of violation and degradation that the victims must have experienced is manifest'. [67]

The jurisprudence is clear that these experiences emphasise the importance of establishing a robust system of privacy protection. As Nissenbaum points out, 'privacy is worth taking seriously because it is among the rights, duties, or values of any morally legitimate social and political system'.[68]

Still, the constitutional right to privacy in SA can be limited. In terms of section 36 of the constitution 'limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors … '.[69] Importantly, the application of section 36 to the right to privacy has been

[63]Irwin Altman, 'Privacy Regulation: Culturally Universal or Culturally Specific?' (1977) 33(3) Journal of Social Sciences, 66–84, 83.

[64]Payal Arora, Decolonizing Privacy Studies, (2019) 20(4) Television & New Media, 366–378, 367. DOI: https://doi.org/10.1177/1527476418806092.

[65]*Mistry v Interim Medical and Dental Council of South Africa and Others* [1998] ZACC 10; 1998 (4) SA 1127 (CC); 1998 (7) BCLR 880 (CC). Judge Sachs, at para 25.

[66]*Gaertner and Others v Minister of Finance and Others* (CCT 56/13) [2013] ZACC 38, at para 1.

[67]*Gaertner and Others v Minister of Finance and Others* (CCT 56/13) [2013] ZACC 38, at para 1.

[68]Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Standford University Press, 2010) at p. 66.

[69]Section 36 of the Constitution reads as follows: 'Limitation of rights (1) The rights in the Bill of Rights may be limited only in terms of 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 into account all relevant factors, including— (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose. (2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights'.

addressed by the Constitutional Court in *Magajane*, where they determined that 'a court has to consider an *applicant's expectation of privacy* [authors emphasis] and the breadth of the legislation, among other considerations'.[70]

In *Gaertner and Others v Minister of Finance and Others* Judge Madlanga elaborated further on the scope of this limitation explaining that:

> as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks. This diminished personal space does not mean that once people are involved in social interactions or business, they no longer have a right to privacy. *What it means is that the right is attenuated, not obliterated*[authors emphasis]. And the attenuation is more or less, depending on how far and into what one has strayed from the inner sanctum of the home.[71]

However, if the scope of private space captured by the right to privacy in South African law extends beyond intimate space, to the social space, in what circumstances will digital interactions be construed as 'straying from the inner sanctum of the home?'[72] And critically, to what extent can an individual have a reasonable expectation of privacy in digital space? There is no doubt that drawing out the boundaries of privacy in South Africa is challenging. Indeed, as Abdulrauf highlights, the jurisprudence on privacy and data protection is still evolving with the majority of case law focusing on the application of the constitutional provision.[73]

Still, in South Africa, privacy can also be protected as part of 'actio iniuriarum'.[74] The Courts have recognised specific categories of privacy invasions that include 'public disclosure of private facts' and 'unreasonable intrusions into the private sphere'.[75] They have also recognised the right to personal identity and of course, protection offered in respect of defamation.[76]

Indeed, the decision in *H v W* provides some very useful insights into the Courts engagement with the challenge of marrying the principled protections to the digital environment.[77] This concerned an action for interdict seeking prevention and removal of postings on a social media network. Highlighting the established common law right to privacy and freedom of expression, Judge Willis emphasised that 'social media … [has] created tensions … in ways that could not have been foreseen by the Roman Emperor Justinian's legal team … or the founders of the constitution'.[78] In his reasoning Judge Willis was clear to highlight the research undertaken by counsel and the influence of the academic commentary upon which he drew. He emphasised the need for such work by explaining that

[70] *Magajane v Chairperson, North West Gambling Board and Others* [2006] ZACC 8; 2006 (5) SA 250 (CC); 2006 (10) BCLR 1133 (CC). At para 50.
[71] *Gaertner and Others v Minister of Finance and Others* (CCT 56/13) [2013] ZACC 38, at para 49.
[72] Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit NO 2001 (1) SA 545 (CC) at 557.
[73] Lukman Adebisi Abdulrauf, Data Protection in the Internet: South Africa, In D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet, Ius Comparatum* – Global Studies in Comparative Law 38, (Springer Nature: Switzerland, 2020) https://doi.org/10.1007/978-3-030-28049-9_14. At p. 351.
[74] Jonathan Burchell, 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 13(1) Electronic Journal of Comparative Law, 1–26, 1.
[75] ibid 9.
[76] ibid.
[77] *H v W* (12/10142) [2013] ZAGPJHC 1.
[78] *H v W* (n77) para 7.

> the pace of the march of technological progress has quickened to the extent that the social changes that result therefrom require high levels of skill not only from the courts … but also from the lawyers who prepare cases such as this for adjudication.[79]

As a consequence of Counsels' preparation, the work of Professor Roos, James Grimmelmann and Neethling were taken into consideration.[80]

Judge Willis relied upon the reasoning of Corbett CJ in *Financial Mail (Pty) Ltd and Others v Sage Holdings Limited and Another* when he explained that

> in demarcating the boundary between the lawfulness and unlawfulness [of an infringement of personal privacy] … [it should be judged] in the light of contemporary boni mores and the general sense of justice of the community as perceived by the Court.[81]

He elaborated that 'Boni mores' means, literally, "good customs/convention" … [which] in this context … may more accurately be translated as "society's sense of justice and fair play"'.[82]

Judge Willis lacked confidence in the ability of the current law (as at 2012) to address privacy infringements in the context of social media arguing that 'the common law needs to develop' and that 'the law has to take into account changing realities not only technologically but also socially or else it will lose credibility in the eyes of the people'.[83] This is important because 'without credibility, law loses legitimacy. If law loses legitimacy, it loses acceptance. If it loses acceptance, it loses obedience. It is imperative that the courts respond appropriately to changing times, acting cautiously and with wisdom'.[84] However, in an environment where 'boni mores' are evolving at pace, any system of regulation will have to be capable of the necessary responsiveness.

Willis agreed with the views of Grimmelmann that 'it is better for the courts to focus on the users rather than [a social network] itself if intrusion on privacy are effectively to be curbed'.[85] He emphasised that this is because 'if one wants to stop wrongdoing, it is best to act against the wrongdoer themselves'.[86] However, Willis expressed some caution arguing that 'it is unseemly for the courts to wield their authority with a sledgehammer'.[87] Nevertheless, he continued to give a warning to social media users that 'those who make postings about others on … social media would be well advised to remove such postings immediately upon the request of an offended party'. He reasoned, 'it will seldom be worth contesting one's obligation to do so'.[88] Rather optimistically he observed 'after all, … social media is about building friendships around the world, rather than offending fellow human beings. Affirming bonds of affinity is what being "social" is all about'.[89] Ultimately, this decision raises concerns because it makes clear that posting on social media is to be considered a form of public dissemination and

[79] *H v W* (n77) para 8.
[80] Anneliese Roos, 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) 129 SALJ 375; James Grimmelmann, 'Saving Facebook' (2009) 94 Iowa Law Review 1137–1205, 1137; Neethling, J. 'Right to Privacy', *The Law of Personality* (2nd ed, LexisNexis Butterworths, 2005).
[81] 1993 (2) SA 451 (A) at 462F -463A cited by Wallis J in H v W (12/10142) [2013] ZAGPJHC 1 at para 29.
[82] *H v W* (n77) para 44.
[83] *H v W* (n77) para 31.
[84] *H v W* (n77) para 31.
[85] *H v W* (n77) para 38.
[86] *H v W* (n77) para 38.
[87] *H v W* (n77) para 41.
[88] *H v W* (n77) para 43.
[89] ibid.

while arguably reducing the scope of an expectation of privacy, increases the potential for material to be considered defamatory.[90]

Since Judge Willis expressed his view, South Africa has taken steps to prepare for the challenges of establishing and protecting these evolving normative expectations. The protection of privacy afforded by the constitution and common law provisions is supplemented by the Protection of Personal Information Act No 4 of 2013 (POPIA). This Act establishes an Information Regulator who is responsible for the monitoring and development of its system of regulating the processing of personal information. In addition, it sets out mechanisms of enforcement that ensure rights attributed to the processing of personal information can be exercised effectively. In SA the first obligation placed on the Information Regulator is 'to provide education', thereafter 'to monitor and enforce compliance', 'to consult with interested parties' – which includes inviting and receiving the views of the public on matters affecting data protection, 'to handle complaints', 'to conduct research and report to Parliament', to produce codes of conduct and guidance, and 'to facilitate cross-border cooperation in the enforcement of privacy laws'.[91]

Although passed in 2013, a number of critical provisions were not brought into force until 2020. This means that the system of regulation, and particularly the enforcement mechanism, has yet to provide decisions that can be drawn upon to consider how privacy boundaries may be interpreted. However, given that regulated entities had until the 1st July 2021 to ensure their compliance we can anticipate an escalation in the enforcement activity of the regulator, albeit that such action is still likely to be hampered by the lack of resources that has limited its progress since its creation.[92]

The POPI Act regulates the processing of 'personal information' where that relates to an identifiable 'living natural person' but also extends to 'identifiable … juristic persons'.[93] This breadth of protection is striking since it means that 'legal persons/entities (like corporations) are also entitled to protection from the processing of their personal information under the Act'.[94] In doing so, it goes considerably beyond the comparable scope of the UK provisions which only apply to 'identified or identifiable living individuals.[95] 'Personal information' is also defined broadly in the SA framework with the indicative list including 'information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language or birth of the person'.[96] In the context of acknowledging the relationship between individuals and the digital environment, it also specifies the inclusion of an email address, location data, and online identifiers.[97] This is in-keeping with the approach taken in the UK

[90]G Mushwana and H Bezuidenhout, 'Social media policy in South Africa' (2014) 19 South African Journal of Accountability and Auditing Research 63–74, 66.
[91]s.40 Protection of Personal Information Act No 4 of 2013.
[92]Rachel Adams and Fola Adeleke, 'Protecting information rights in South Africa: the strategic oversight roles of the South African Human Rights Commission and the Information Regulator' (2020) 10(2) International Data Privacy Law 146–159, 155.
[93]s1, Protection of Personal Information Act No 4 of 2013.
[94]Lukman Adebisi Abdulrauf, Data Protection in the Internet: South Africa, in D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet, Ius Comparatum* – Global Studies in Comparative Law 38, (Springer Nature, 2020). DOI: https://doi.org/10.1007/978-3-030-28049-9_14. At p. 354.
[95]s3(2), Data Protection Act 2018. c12.
[96]s1, Protection of Personal Information Act No 4 of 2013.
[97]s1, Protection of Personal Information Act No 4 of 2013.

framework although, the UK provision is less descriptive providing only that personal information means 'any information relating to an identified or identifiable living individual'.[98] That being said, it too felt the need to offer some clarification of its applicability to the digital world as it explains that to be 'identifiable' would include 'location data or an online identifier'.[99]

In SA obligations are placed on 'responsible parties' who are 'public or private [bodies] or any other person, which alone or in conjunction with others, determines the purpose of and means of processing personal information'.[100] However, it is restricted to those who are domiciled in the Republic or in circumstances where they make use of automated or non-automated means in the Republic.[101] In order for data to be 'lawfully processed' the responsible party must meet conditions on accountability, processing limitations, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation.[102] There are some limited exceptions to these conditions in that they will not apply to data processed as part of a personal or household activity or to data that has been de-identified provided it is not capable of being re-identified.[103] Both of these exclusions are important in the context of regulation privacy boundaries in digital space. Interactions between individuals in a social context will often not be protected by the operation of the conditions for lawful processing falling outwith the scope of regulated data. However, the exclusion of information which has been re-identified is likely to gradually reduce in scope as advances in technology increase the potential for re-identification, meaning less data will escape regulation.[104] For example, there is already research that indicates how new and radical approaches can be used to re-identify an individual.[105]

In the UK, the right to privacy is principally secured through the Human Rights Act 1998 and the Data Protection Act 2018.[106] These legislative provisions are complemented by a range of common law and statutory provisions, which articulate how the boundaries of privacy have been established in law.[107] The Data Protection Act 2018 was specifically designed to update the law to ensure that it was fit for the 'digital age'.[108] This was because both the UK economy and society is ever more digital with 'personal data … increasingly stored, processed and exchanged on the internet'.[109] Specifically, it was recognised that disclosure of personal data has the potential to cause harm and consequently the legislation requires that controllers 'design and organise their security to fit the nature of the personal data that they hold and the harm that may result from a

[98]s3(2), Data Protection Act 2018. c12.
[99]s3(3)(a), Data Protection Act 2018. c12.
[100]s1 and s3(a), Protection of Personal Information Act No 4 of 2013.
[101]s3(b), Protection of Personal Information Act No 4 of 2013.
[102]s4(1)(a)-(h), Protection of Personal Information Act No 4 of 2013.
[103]s6(a) and (b), Protection of Personal Information Act No 4 of 2013. There is also an exclusion in respect of data processed by or for a public body in relation to issues of national security or crime control as well as for Government Ministers and judicial functions of courts but discussion of these is beyond the scope of this work. s6(c), Protection of Personal Information Act No 4 of 2013.
[104]Veliz (n4) 20.
[105]Ron S. Hirschprung, Ori Leshman, 'Privacy disclosure by de-anonymization using music preferences and selections', (2021) 59 Telematics and Informatics 101564.
[106]Article 8, Schedule 1, Human Rights Act 1998, c42.
[107]Elspeth Reid, Protection for Rights of Personality in Scots Law: A Comparative Evaluation, (2007) 11(4) EJCL 1-36,1.
[108]Explanatory Notes to The Data Protection Act 2018, c12., para 1.
[109]Explanatory Notes to The Data Protection Act 2018, c12., para 5–6.

security breach'.[110] Indeed, where a breach occurs which has the potential to cause 'serious harm' it has to be reported to the Information Commissioner.[111]

The UK have implemented similar provisions to SA albeit with some important distinctions.[112] Focusing then on Part 2 of the Data Protection Act, it applies to 'controllers' who are 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data' and 'processors' who are 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.[113] Importantly, as with the SA provisions, there are exclusions to its scope. It will also not apply to data processed 'by a natural person in the course of a purely personal or household activity'.[114]

The Information Commissioner's Office has been established in the UK since 1984 over that time its role and responsibilities have evolved. In terms of the current regulatory framework, it is responsible for 'monitoring and enforcing compliance', 'promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to processing', 'encourage the drawing up of codes of conduct' and 'approve binding corporate rules' amongst other obligations.[115]

In terms of sanctions and remedies, the ICO has the ability to issue enforcement notices that instruct a person to take specific steps or to refrain from particular actions.[116] Where there is a failure to comply with any notification from the ICO, they can issue a penalty notice.[117] The maximum amount of penalty varies considerably depending on the nature of the failure. However, to provide one illustrative example, where the matter concerns a breach of the basic principles for processing the fine can be up to 20,000,000EUR or 4% of an undertakings annual turnover.[118]

An individual who wishes to assert their data protection rights can do so by lodging a complaint with the ICO or raising civil proceedings.[119] Significantly, there is also the opportunity for an individual to be represented by a non-profit body or organisation with their consent.[120] Although the UK GDPR allows scope for rules to be introduced which would enable action to be taken even without consent, no provisions have been proposed. This may be a reflection of the fact that there are pre-existing provisions, such as the English civil procedural rules, which allow for a representative action to be taken (on behalf of a group) although there are restrictions:[121] That group must have the same interests and the group must be sufficiently identified.[122] Importantly, the

[110]Explanatory Notes to The Data Protection Act 2018, c12., para 189 and 256.
[111]Explanatory Notes to The Data Protection Act 2018, c12., para 279. Article 33 General Data Protection Regulation 2016/679 OJ L 119, S67, S108 Data Protection Act 2018, c12.
[112]In contrast to the SA framework, the UK legislation capture the regulation of state and non-state actors including those involved in the prevention and detection of crime and national security, although in separate chapters. There is no doubt that there are significant privacy implications in respect of those activities but there is not sufficient space to fully address them within this paper.
[113]s5 Data Protection Act 2018. c12.
[114]s4(2)(a) Data Protection Act 2018. c12.
[115]s115(2)(a) Data Protection Act 2018. c12.
[116]s149 Data Protection Act 2018. c12.
[117]s155 Data Protection Act 2018. c12.
[118]s155(2)(a) Data Protection Act 2018. c12.
[119]Article 77 & Article 79, GDPR.
[120]Article 80, GDPR.
[121]Civil Procedural Rules R19.6.
[122]*Emerald Supplies* [2011] CP Rep 14. Mummery LJ at para [62]–[65].

court emphasised that 'the number of claimants cannot itself affect the ability to use the representative procedure'.[123] And significantly, the members of that group do not have to have individually agreed for the representative action to continue.[124] However, the position is different across the UK, with the Scottish measure only facilitating an opt-in consent-based procedure.[125]

In SA the Information Regulator is bound to establish an Enforcement Committee and that Committee will consider matters referred to it by the Information Regulator following an investigation. It will be required to provide a recommendation for its disposal to the Information Regulator.[126] It is the Information Regulator who has the authority to issue sanctions where those sanctions include an enforcement notice which can detail actions that have to be taken (or ceased) by the responsible party.[127]

The Regulator has the authority to issue administrative fines to a maximum of R10million (approximately $678,790.00).[128] Importantly, in considering the level of fine, the Regulator should take into account 'the likelihood of substantial damage or distress, including injury to feelings, or anxiety suffered by the data subject'.[129] Administrative fines and criminal proceedings cannot be pursued on the same set of facts, but a civil action could be.[130] Group rights or representative actions are surprisingly limited. The Regulator appears to be the mechanism through which groups of data subjects would pursue sanctions as opposed to being able to directly access the courts as in the UK system. This is particularly surprising in the context of SA because it would be more in-keeping with collective ideals to facilitate a mechanism by which a 'community' of data subjects were able to pursue action.[131]

That being said, the constitution expressly facilitates the ability of class actions and representative actions.[132] And, so it may be that the draughters of POPIA anticipated that actions asserting an infringement of data protection (as a part of either the right to privacy or the right to dignity) could be addressed through this route and that this would preserve the cultural integrity of privacy protections.

6.3. The rise of responsibilisation

It is clear that in the UK and South African systems, a predominantly regulatory approach has been adopted to data privacy. In doing so, they have furnished non-state entities with powers of enforcement and responsibilities for increasing awareness of rights protections. Responsibilisation is not a new phenomenon. It has been widely deployed through the outsourcing of regulatory functions, particularly in the field of policing.[133] In both jurisdictions there has been engagement with stakeholders that has facilitated the incorporation

[123] *Lloyd v Google LLC* 2019 WL04804855. Sir Geoffrey Vos C, at para 80.
[124] See *John v. Rees* [1970] Ch 345 , per Megarry J at 371.
[125] Chapter 26A, Court of Session Rules.
[126] s92 Protection of Personal Information Act No 4 of 2013.
[127] s95 Protection of Personal Information Act No 4 of 2013.
[128] s109(2)(c) Protection of Personal Information Act No 4 of 2013.
[129] s109(3)(e) Protection of Personal Information Act No 4 of 2013.
[130] s109(6)-(7) Protection of Personal Information Act No 4 of 2013.
[131] Olingera et al (n22) 33.
[132] S38, Constitution of the Republic of South Africa 1996.
[133] Mo Egan, 'Policing intermediaries in the EU anti-money laundering framework', (2016) 4(1) Special Issue: Policing in Times of Uncertainty, European Journal of Policing Studies 125–145, 132.

of their views into the creation of codes of conduct. As a result, these stakeholders are able to influence where privacy boundaries are established and how they are evaluated. And, while there are clear practical reasons why engagement with stakeholders is critical, given their privileged knowledge about how they are processing data, it also brings with it risk to individual privacy.

For example, although in SA the regulator is only required to consult with stakeholders as it stands the codes of practice that have been published to date have all been proposed by specific organisations or stakeholder representatives.[134] Of particular interest for our purposes is the Code of Conduct produced by Willcom (PTY) Ltd, a company in the telecommunications and information technologies industry. While purporting to be compliant with the provisions of POPIA, it simultaneously provides qualifying language. It explains that

> [t]he provisions governing the processing of information in the Company, *while not as extensive* [author's emphasis] as PoPIA, are not inconsistent with PoPIA and the Company complying in this regard will *largely* [author's emphasis] comply with the conditions for the lawful processing of personal information contained in PoPIA.[135]

However, there is another aspect of responsiblisation that deserves acknowledgement: Both systems shift responsibility to individuals. Individuals are responsible for taking steps to protect their privacy. Individuals are expected to engage with privacy mechanisms and where they fail to do so, it may impact on the availability of remedies. Individuals are expected to participate in the policing of privacy violations through various reporting mechanisms.

7. Conclusion

Altman and Hughes offer a robust framework for understanding how privacy barriers manifest in human interactions. However, marrying this practical reality with normative validity is complex. Developing a system with sufficient cultural flex to ensure legitimacy of formal regulation is problematic. It is problematic because there are competing cultural dynamics between those cultural expectations anchored in particular jurisdictions and evolving digital cultures. In the UK and South Africa there is some recognition of this challenge in that they have each adopted a system of data protection regulation that seeks to responsibilise both non-state actors and individuals. In the case of non-state actors this is achieved through the development of codes of practice and in the case of individuals this is achieved through the promotion of media literacy. In each of these examples, it is possible for the regulatory framework to be responsive to the needs of digital society.

That being said, the UK is likely to be impeded in it progress as a result of exiting the EU. With the UK Data Protection Act fundamentally based on the EU framework, many of its provision either implement directly or only make minor alterations to that framework.

[134]Notice in Terms of S61(2) of the Protection of Personal Information Act No 4 of 2013 Code of Conduct: Credit Bureau Association, April 2021; Notice in Terms of S61(2) of the Protection of Personal Information Act No 4 of 2013 Code of Conduct: Rocketjumper Birding Tours Ltd, Government Gazette No44881, 23 July 2021; Notice in Terms of S61(2) of the Protection of Personal Information Act No 4 of 2013 Code of Conduct: Willcom (PTY)Ltd, Government Gazette No44881, 23 July 2021;

[135]Para 10.8. Code of Conduct Governing the Conditions for Lawful Processing of Personal Information By Willcom (PTY) Ltd. Issued in Terms of S60 of the Protection of Personal Information Act, No. 4 of 2013 By the Information Regulator.

With the UK recently voicing their intention to leave the GDPR, they would be well advised to remain cautious about alterations.[136] This is critical because the extraterritorial effect of the GDPR is such that if the UK wish to remain trading partners with the EU, they will have to demonstrate that they provide a system of protection that is equivalent. However, with the Culture Secretary suggesting that this move would enable the UK to remove 'box-ticking' exercises such as cookie pop-ups and consent requests and instead rely upon 'common-sense' equivalence looks open to debate.[137]

In South Africa, the lack of empirical work assessing the prevalence of privacy harms needs to be addressed. The need for robust research is important to be able to ensure that the expectation of individuals in digital space is compatible with the current approach to regulation and where it is not, to consider whether it is time for formal regulation to evolve. At the institutional level, with the Information Regulator in its infancy, it requires the appropriate resources to ensure that it is in a position to effectively enforce the protective measures. Moreover, at the individual level, there is still some cause for concern in that its ICT infrastructure still lags behind other jurisdictions. This is problematic in that it inhibits an individual's ability to participate in digital society and thus fosters a potential for dissonance between an individual's expectation of privacy and its practical attainment. Indeed, as comprehensive as Altman and Hughes accounts are, neither address the structural social and economic barriers that may inhibit an individual ability to decide to erect a privacy boundary, the means by which that can be achieved, and the money to make that happen.

Disclosure statement

No potential conflict of interest was reported by the author(s).

[136]Alex Hern, 'UK to overhaul privacy rules in post-Brexit departure from GDPR', The Guardian, 26 August 2021.
[137]ibid.