POLICY BRIEF 05

MANDELA INSTITUTE

COMPETITION POLICY AND DATA PROTECTION IN AFRICA

Jonathan Klaaren

MANDELA INSTITUTE, SCHOOL OF LAW,
UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

CONTENTS

1.	Introduction	1
2.	The policy domains of competition and data protection	2
3.	The interacting issues of competition policy and data protection	3
4.	Relevant African regulatory capabilities and developments	4
5.	Data localisation, competition policy, and data protection	5
	5.1 Africa	5
6.	Conclusion	7
Endnotes		8

1. INTRODUCTION

This policy brief forms part of a broader collection of work on the economic impact in Africa of data protection through data localisation. This work is pertinent as African states adopt privacy regulation at a national level and as developments on a regional level also ramp up. Topics covered in this collection of work include: regulating Africa's digital economy and the emerging policy considerations, African free trade and data protection, cross-border digital flows and data protection, and regional impacts of data localisation. The policy brief draws on several country reports detailing policies in Kenya, Nigeria and South Africa which assist to identify ongoing regulatory developments.[1]

The focus of this policy brief is on competition policy and data protection. The second section of this brief first sketches each of these policy domains at the African level. The third section then examines the interaction of these two policy domains at the global level, identifying a number of priority issues that sit at the intersection between these two policy domains. These issues include data portability and interoperability, and the section investigates, further, the former. The fourth section turns to the African regulatory capabilities in these domains, briefly surveying both regulatory capacity and recent policy discussions. The fifth section describes and examines the current moves towards data localisation in Africa from the continent-wide perspective gained regarding data portability.

2. THE POLICY DOMAINS OF COMPETITION AND DATA PROTECTION

In order to specify the policy domain of competition, one must begin by noting the significant difference between a narrow focus on competition law and a broader focus on competition policy. The former, especially when understood narrowly, can mean a focus on a jurisdiction's competition statute (if any) and its enforcement. The latter, especially when taken on board by industries and government institutions beyond the realm of the competition authorities, encompasses studies of industrial policy, economic regulation, development, and innovation.

Understood in the above sense, the African competition policy domain includes, but is not limited to, the national and regional competition laws providing for enforcement action by African competition authorities. Even judging by the narrow measure of national legislation, the policy domain is fairly well consolidated in Africa. Already in 2015, the World Bank had reported 27 African countries with competition laws enacted.[2] Four years later, the Economic Commission on Africa counted 33 African countries with a competition law in place.

A recent development within the policy domain of competition, which is a growing focus of competition policy, is that of inequality. For instance, in a recent conference paper, Cachalia and Beyleveld explored to what extent distributional considerations could, and arguably should, inform the development and implementation of competition law and policy in South Africa.[3] They noted recent research that has highlighted the ways in which deviations from perfect markets may contribute to rising economic inequality, as well as other research on the competition inequality nexus, generally from the perspective of market power and the resulting market rents that accrue predominantly to the wealthier segments of society. Cachalia and Beyleveld register that competition policy does not operate in a vacuum and therefore explore other options for reducing economic inequality and how these might and/or should interact with a competition law and policy that seeks to address distributional concerns.

In order to specify the policy domain of data protection, one might usefully begin with a recent survey made of the formal commitments garnered by a series of data protection legal instruments relevant for Africa.[4] Comprehensively examining African jurisdictions and their data protection laws and policies as of 2020, Greenleaf and Cottier have argued that Africa is currently 'leading [the] global expansion, with 12 countries since 2013 adopting new laws'.[5] They note that 32 of 55 African countries had enacted data protection laws as at February 2020 and that African countries have been regularly enacting data privacy law for nearly 20 years.

Regardless of its consolidation, as with the competition policy domain and indeed all such domains, the data protection field in Africa remains subject to change. To take one relevant aspect, while the public law of privacy clearly touches upon the data protection policy domain, that legal topic has yet to become a fully constitutionalised field. For instance, in a forthcoming working paper on the constitutional right to privacy in South Africa, Cachalia and Klaaren have explored what normative resources there might be in South Africa's post-apartheid legal system to develop a 'public law perspective' on privacy law that can recognise and exert some control over commercial and collective harms associated with digitalisation as well as individual ones. They argue that South Africa's unique version of transformative constitutionalism provides ample conceptual, normative and institutional resources to develop a constitutionalised privacy jurisprudence fit for the age of 'Surveillance Capitalism' and the 'Surveillance State'.

3. THE INTERACTING ISSUES OF COMPETITION POLICY AND DATA PROTECTION

The interaction of competition policy and data protection is a topic on its own. Since 2019, the world has witnessed an explosion of attention to these issues on the part of economies around the globe. Many nations and some supra-national regions (such as the European Union) (EU) are now publicly investigating and debating potential new governmental controls of these tech giants. These efforts are having ripple effects throughout the globe and are influencing regulatory initiatives in non-OECD (Organisation for Economic Co-operation and Development) countries as well.[6]

The bulk of these efforts are unfolding in the Global North and differ significantly among themselves. In the United Kingdom, a preliminary investigation held by the competition authority reported in June 2019 and was followed by a high-profile commission, the Furman Commission.[7] In the United States (US), the issue of big tech has registered in presidential campaigns, in congressional hearings, and in announcement of antitrust investigations by agencies of the federal government. In Germany, the competition authority found against Facebook in 2019 on the theory of abuse of dominance for amassing data and violating privacy laws.[8] In Australia, the Australian Competition and Consumer Commission announced the findings and recommendations of its digital platforms inquiry in July 2019.[9]

As these initiatives have progressed, a number of common issues have emerged. These common issues include (but are not limited to): price discrimination, Most-Favoured Nation clauses, self-favouring, data portability, data localisation, interoperability, exclusivity clauses, user lock-ins, and access to business user-generated data. While space does not permit close examination of each of these issues, a deeper dive into at least one of these globally significant issues – data portability – is worth pursuing here.

One might even argue that the issue of data portability has become a policy domain distinct from those of data protection and competition policy. Its main line of distinction from the privacy paradigm embedded within the field of data protection is to present an alternative to the notice-and-consent rules that have historically featured prominently in safeguarding privacy, ideally requiring the collectors and users of data to work with the parameters of explicit and specific permissions gathered from the data subjects. Such a notice-and-consent model, however, breaks down in the era of digitalisation, where data collection is continuous and the uses for data are non-obvious and sometimes completely novel. Some advocates, particularly within advanced digital societies with relatively minimal privacy regulation, have produced draft legal instruments focusing solely on data portability.[10] In an indication of the significance of the subject matter, five of the big tech companies – Google, Facebook, Twitter, Apple and Microsoft – joined forces in 2018 to launch the Data Transfer Project 'to create an open-source, service-to-service data portability platform so that all individuals across the web could easily move their data between online service providers whenever they want'.[11]

Within the data protection/privacy realm, some specific steps have been taken towards strengthening data portability in the EU and, at the state level in the US, in California. As many African Internet users will have no doubt noticed, these changes in law in these specific jurisdictions have had some effects globally. Article 20 of the General Data Protection Regulation (GDPR)[12] and some provisions of the new California Privacy Law take some steps beyond a notice-and-consent model to protect the privacy of consumers and move towards enhancement of data portability.[13] Still, both the new GDPR and the new California legal forms are effectively weak forms of what one may term[14] (and they do) the right to data portability.[15]

> The strong form of a right to data portability rooted in a competition-based policy paradigm has several specific differences from the weak form of the right to data portability.

Within the realm of competition and antitrust, it is worthwhile to look at the recent Australian public debate on data portability. Proposals have been put forward by the Australian Competition Commission which may be termed a strong version of the rights-based data portability approach. The mooted Australian policy perhaps goes furthest of the developed country jurisdictions by introducing a consumer data right, not a right of property ownership but a right resulting in the sharing of data between data subjects and data holders.[16]

The focus on consumer data in these Australian proposals reveals an important difference between the conceptual routes of competition policy and data protection in dealing with issues at their intersection. As Beaton-Wells puts it in discussing the Australian competition proposals:

> *At the heart of this model is a basic distinction drawn between privacy and competition as each*

relates to consumer data. While privacy focuses on managing data use by others, the CDR [consumer data right] focuses on enabling consumers themselves to control its use. In essence, the distinction is between limitation or aversion of a threat (to which privacy policy is directed) and opening up and spreading of opportunity (to which competition policy is directed). Drawing the distinction allows for the narrative surrounding data to be changed, from one concerned with harms to one concerned with benefits.[17]

The strong form of a right to data portability rooted in a competition-based policy paradigm has several specific differences from the weak form of the right to data portability. Without being comprehensive, three are of particular interest here. First, the rights-holders include firms as well as individuals. This allows for small enterprises to assert their rights against large firms holding data as well as to improve the dynamics of competition among firms within these markets. Second, the data covered by the strong form as individualised data includes associated data (e.g. data not directly provided by the individual but gathered or accessed from elsewhere in relation to that individual) as well as directly provided data. This means that a consumer has power over a much greater range of data linked to them as an individual. Third, the right proposed is strong enough to empower 'consumers to have access to and control over their data, enabling them to have it transferred by the data holder to an accredited third party at their direction, and in a form that is digitally practicable'.[18]

Two academics writing in one of the top-ranked law journals in the data protection field have surveyed the recent policy development regarding data portability rights in Australia.[19] They view these rights as a significant legal innovation with the potential to stimulate the development of digital economies. Burdon and Mackie note that the main form of implementation of the consumer data right in banking, telecommunications, and energy sectors has taken the form of mandated application programming interfaces (API). An API is a bit of software that allows two (or more) applications to communicate with each other.

Burdon and Mackie further argue that the role of informational privacy within the data portability framework in Australia has significant areas of uncertainty, largely derivative of the conflict in goals between competition and privacy frameworks. In their view, noting that the legal instrument for the CDR has a separate set of privacy standards from those of the Australian Privacy Act, 'the judicial categorisation of data types in both schemes [has a risk to] depart in different directions which could further weaken the already limited coherence of the *Privacy Act's* comprehensive focus'.[20] Advocating for a privacy-centred view of the policy issues, Burdon and Mackie hold that 'privacy is not a bolt-on. Instead, it is a foundational protection that requires careful consideration, including in a competition law focussed data portability scheme'.[21]

4. RELEVANT AFRICAN REGULATORY CAPABILITIES AND DEVELOPMENTS [22]

While the previous section largely took a global perspective, this one refocuses on the African continent and the jurisdictions and economies found there. Currently, we can say that there are some teeth (and considerable potential) in African competition regulatory agencies[23] and somewhat less in African information/privacy regulators.[24] This section investigates the capability of the regulatory regimes at the relatively simple level of the number of functioning regulators. This investigation takes the enquiry a step beyond the identification of regulatory instruments, which was the method for identifying the contours and dynamics of the competition and data protection policy domains in section two above.

We can count 12 information/privacy regulators as of 2018 (with another three established in law but not yet operational) as compared with 32 competition regimes as of 2015 (27 national and five regional). Similarly, while Sutherland only identified one functioning digital privacy governance network among the West African region at the African level in 2018, there are functioning networks for nearly every African region in the competition domain as well as an overarching coordinating body at the continental level, the African Competition Network.[25]

So, what are these (and other) African regulators doing? The regulatory response to the intersecting issues of competition policy and data protection in Africa is best characterised as at the policy paper stage. Barely more than a month apart, government entities within two of Africa's leading economies – Kenya and South Africa – have published policy papers on the digital economy and its impact on their nations and have asked for public comments. The Ministry of Information, Communication, Technology, Innovation and Youth Affairs in Kenya published its 60-page Digital Economy Strategy Draft 1 in July 2020.[26] Comments on this draft were open from 7 August and were due by 28 August 2020. The Competition Commission (South Africa) published its 68-page policy paper Competition in the Digital Economy on 7 September 2020, asking for comments by 30 October 2020.[27]

These two papers purport to cover much of the same ground. Kenya's document examines digital govern-

ment, digital business, infrastructure, innovation-driven entrepreneurship, digital skills and values, digital inclusion, and cross-cutting issues. The South African one looks at digital platforms in South Africa, competition law in digital markets, regulatory issues in the digital economy, and even the impact of COVID-19 on the digital economy. As reflected, inter alia, in their titles, both papers also take a whole-economy rather than a sector-specific or even set-of-sectors approach to the topic.[28]

There are significant differences, however, both in terms of audience/purpose as well as subject matter. The Kenyan policy stems from the May 2019 Transform Africa Summit, the flagship event of the SMART Africa Alliance, Kenya being the champion for the Digital Economy pillar within that Alliance. According to the Ministry, the strategy was 'developed collaboratively between the private and public sector and it is envisioned that its implementation and realisation will require the same collaborative process'.[29] The South African one is owned very much by the Competition Commission and has a more limited set of aims – to inform government and corporate stakeholders of the Commission of the Commission's views on competition in the digital economy and, perhaps just as importantly, 'to inform South African regulators of the Commission's position on the digital economy to facilitate coordinated regulatory and advocacy efforts in this area'.[30]

> The regulatory response to the intersecting issues of competition policy and data protection in Africa is best characterised as at the policy paper stage.

As one might expect from documents issued by, on the one hand, a competition authority and, on the other, a Ministry of Information, Communication, Technology, Innovation and Youth Affairs, the prominence of competition law and policy is a significant difference. Kenya's document mentions competition but twice – once to include 'fair competition' as part of digital business and a second time to see the digital economy as enhancing Kenya's competition in the global economy. South Africa's document is authored by the competition authority and uses that policy lens primarily. After a first descriptive section, the remaining two substantive sections cover, in sequence, competition law and regulation, replicating the usual competition authority plus economic regulator conceptual approach of competition authorities worldwide. The discussion of competition law and policy is split into standard categories of cartels, abuse of dominance, and merger regulation. Data portability is mentioned but once in the South African document (at 55) in the context of promoting inclusion in financial services and mentioned not at all in the Kenyan text. In this respect, the South African document notes the Australian recommendation for the CDR but does not take a position on that policy recommendation.[31]

These policy documents reflect the recent history of policy development and regulatory action for these two leading African jurisdictions. Within the competition domain, the voice of the telecommunications regulator is more prominent than that of the competition authority of Kenya (one of the strongest competition authorities in Africa) on the risks and opportunities in the development of the digital economy in Africa. In South Africa, the official pronouncements of the competition authorities are effectively aligned with the views on digital markets expressed globally. The December 2019 Data Services Market Inquiry confirmed the high South African prices for data, relative to global and African standards, and made several recommendations re MTN and Vodacom, to be put into various legal and policy processes.[32]

Perhaps more significantly, the competition authorities have been part of a process of formulating South African national industrial policy, titled Towards a Digital Industrial Policy (17 July 2019). The publication from this process observes:

> *Online platforms have the potential to open-up routes to consumers for small, medium and micro enterprises (SMMEs), by lowering entry barriers. But, at the same time, the platforms have substantial market power and can skew the playing field. These tensions are evident in the ways in which e-commerce is changing the face of retail internationally.*[33]

According to the publication

> *[d]igital technology policy needs to be integrated with industrial policy and should include measures such as the provision of manufacturing and digital extension services, demonstration projects, and testing and scaling-up facilities such as accelerators for digital start-ups and SMMEs.*

In addition to calling for appropriate regulation for digital platforms to ensure the playing field is level for local businesses, the report is clear that South Africa needs to develop a clearly defined set of policies on data ownership, data quality, data categorisation and de-identification.

5. DATA LOCALISATION, COMPETITION POLICY, AND DATA PROTECTION

This section concludes the policy brief by examining more closely the particular issue area of data localisation on the African continent from the perspective of competition policy and data protection.

The fast-emerging issue area of data localisation may be seen as a counterpoint to that of data portability, identified and discussed above. Indeed, the comparison is a worthwhile one to outline, at least in brief along several dimensions. In data localisation, the policy movers appear to be sovereign jurisdictions at the national level. In data portability, the policy movers appear to fall within a broader range and include sub-national jurisdictions, large technology corporations, and non-governmental organisations (NGOS) as well as national governments. Not surprisingly, the degree of transnationalisation appears limited for data localisation but to be significant for data portability. Comparing the conception of privacy protection through the mechanism of notice-and-consent requirements, data portability regards itself as an alternative, while data localisation continues to work with these requirements, although they do not appear to be prominent. The dominant discourse for data localisation is that of sovereignty (data or digital sovereignty[34]) – while that for data portability is individual rights (data or digital rights). Interestingly, both policy areas would claim to be advocating open access and open data. The legal instrument used for regulation also differs – for data portability, technical standards are perhaps the foundational locus, while data localisation depends on national legislation. Arguably, the prime regulatory body for data localisation remains tele-communications regulators while for data portability the lead agencies appear to be consumer protection bodies.

5.1 Africa

At the African policy level, data localisation enjoys a higher profile than does data portability. Part of the African Union's Agenda 2063, the Digital Transformation Strategy for Africa (2020), discusses data localisation in secondary yet significant terms:

> *The main benefit of … infrastructure localisation [including data centres] on the continent will be cost savings on international connectivity and the latency decrease that will deliver a better application performance. The second interest [underlying the importance of infrastructure localisation] is respect for data sovereignty, even though Africa is at the moment less restrictive, soon it will be necessary to ensure localisation of all personal data of Africa's citizens.*[35]

A specific proposed action endorsed by this policy document as part of strengthening cybersecurity at national level is to 'adopt a law on the localization of data with respect for the privacy of African citizens and residents'.[36] Portability (rather than the more specific term 'data portability') is mentioned only once by the African Union in the context of a recommendation on access to health information: 'Create a continental standard for the portability and accessibility of medical information to be adhered to by Member States.'[37]

5.1.1 Nigeria

One Nigerian administrative agency, the National Information Technology Development Agency (NITDA), has pushed for data localisation by means of several legal and policy instruments.[38] In terms of a 2013 policy, telecommunications and network service companies are required to host all subscriber and consumer data in Nigeria.[39] This policy also made further provision that all ministries, departments, and agencies in Nigeria host websites locally and under a registered '.gov.ng' domain.[40] Similarly, all data and information management companies must host all sovereign data in Nigeria,[41] and ministries, departments and agencies must host all sovereign data on local servers within Nigeria.[42] Further, in terms of a 2019 NITDA policy on cloud computing, the ministries, departments and agencies may only use cloud computing in jurisdictions with data protection regimes at least equivalent to those of Nigeria. Other regulatory measures conducive to data localisation have been taken by the Nigerian Communications Commission and the Central Bank of Nigeria, with perhaps the most significant being the content of the pending data protection legislation.[43]

5.1.2 Kenya

In Kenya, data localisation requirements are laid down in section 50 of the Data Protection Act of 2019 and Regulation 25 of the proposed Data Protection (General) Regulations 2021. Kenya's data localisation and, at least to a certain extent, the broader data protection frame-works are not yet settled. The proposed general regulations containing the data localisation provisions are currently under consideration after a public-participation exercise that ended on 11 May 2021.[44] A review of the proposed regulations indicates that Kenya is leaning towards strict data localisation measures. Regulation 25 proposes data localisation measures that require companies operating in the Kenyan economy to store and process data locally using data centres located in the country, that ban cross-border sensitive data transfers, and that require the fulfilment of certain conditions before the implementation of any transfer of data abroad.[45]

It has been argued that Kenya has been running high risks with its incomplete data protection framework.[46] The case law decided by Kenyan courts based on the privacy rights afforded in the Kenyan Constitutions (the old and new) has been assessed as inadequate for the purpose of privacy protection. Makulilo and Boshe have thus argued that Kenya 'risks losing business opportunities from foreign investment … because the existing legal framework does not afford adequate protection'.[47]

5.1.3 South Africa

South Africa has a proposed National Data and Cloud Policy out in first draft form with the period for comment now closed.[48, 49] In its rationale for this policy, the South African government states:

> *... the national agenda of government seeks to accelerate interventions aimed at unlocking investment opportunities, ensuring inclusive economic growth, and job creation... The Data and Cloud Policy seeks to strengthen the capacity of the State to deliver services to its citizens, ensure informed policy development based on data analytics, as well as promote South Africa's data sovereignty and the security thereof.*[50]

The proposed policy was published by the Minister of Communications and Digital Technologies and is wide-ranging.[51] For instance, it occupies in part the policy space on the classification of information held by the state, a space formerly taken up by the Protection of Information Act, a piece of legislation approved by Parliament, subject to strenuous constitutional objections and two referrals, and currently (and for the foreseeable future) stalled in the Presidency under the constraints of section 79 of the Constitution.[52] This draft appears to presume the validity of that bypassed and much-maligned piece of legislation and proposes in policy intervention 10.3.5 that '[t]he Minimum Information Security Standards and Protection of State Information Legislation shall be reviewed, where necessary, to enable protection of sensitive data in the digital economy.'[53] In this same vein, the policy treats the vexed issues of cybersecurity within the paradigm of national security risk management.[54] In another example of its breadth, the policy appears aligned with the recent paper of the Competition Commission and also proposes a review of competition legislation in the service of building a digital economy.[55] At the same time, the policy plans to merge regulatory entities and also to merge some state-owned enterprises (e.g. Sentech and Broadband Infraco) to establish a state-owned network – a prospect greeted with scepticism by some commentators.[56] Key discursive themes of the policy include state data ownership and data localisation.[57] Indeed, the policy has come under fire as a 'digital grab', with concerns being expressed from both privacy and property rights points of view.[58] The parts of the proposed policy heavy on state intervention can be seen as an example of what Anthony Butler has argued is an over-reliance on state capability in South Africa, noting the current official interest in the work of the economist, Mariana Mazzucato.[59]

Perhaps revealing its greater familiarity with data protection policy than with competition policy. The draft policy defines data portability as 'the right of the data subject to obtain data that a data controller holds on them, and such data is in a structured, commonly used and machine-readable format, and to re-use it for their own purposes.'[60] The only non-sourced use of the concept, however, comes in the presentation of policy interventions flowing from the engagement with competition questions.[61] Here, data portability is understood as one of a number of sub-elements (perhaps linked to the sub-element of interoperability) of a proposed governmental adoption of an Open Data Strategy. For this policy, data portability appears to operate mostly among and at the level of cloud providers, where the policy makes the sensible suggestion of greater reliance on open-source standards.

> The legal instrument used for regulation also differs – for data portability, technical standards are perhaps the foundational locus, while data localisation depends on national legislation.

Consistent with the AU Agenda 2063 document, the draft Cloud and Data Policy sees data centres and infrastructure within a digital economy as the starting points for discussing data localisation which is teamed up with cross-border data flows.[62]

The Cloud and Data Policy adopts a position clearly welcoming data localisation. Three policy recommendations contained in the document make this clear. First, all data classified/identified as critical information infrastructure must be processed and stored within the borders of South Africa. Second, cross-border transfer of citizen data may only be carried out by adhering to South African privacy protection policies and legislation (POPIA) and the provisions of the Constitution, and in compliance with international best practise; this, notwithstanding, a copy of such data must be stored in South Africa for the purposes of law enforcement. Third, '[t]o ensure ownership and control: [d]ata generated in South Africa shall be the property of South Africa,

regardless of where the technology company is domiciled'.[63] The policy was open for comment after its 1 April 2021 publication and has been subjected to a number of cogent criticisms.[64]

Indeed, while touching on tax issues, the policy discussion on localisation and the draft Cloud and Data document more generally does not engage with the data, arguments, and provisional policy positions developed on behalf of South Africa by the DTIC-funded Industrial Development Think Tank.[65] This body of research has made two key proposals in respect of data localisation and data portability: (a) that localisation of data should only be enforced on a case-by-case basis for strategic sectors; and (b) that South Africa should develop a data-governance regime, which must prioritise interoperability and portability of data, and privacy protections (and, further, prioritise data-governance regulations for consumer data in healthcare, tele-communications; online search and location data; and financial and transactions data).[66]

6. CONCLUSION

The development of these policies provides the opportunity to canvas a number of perspectives and to ask some probing questions. One cross-cutting question that ought to be posed to those formulating polices of both data portability and data localisation is whether the policy contributes to digital equality and data justice. From a global perspective, such as that taken by the global development organisation UNCTAD (which is currently preparing a discussion paper on cross-border data flows), what should good cloud and data policy prioritise? Are the priorities the same for developing countries as they are for OECD countries with advanced economies and fiscal strength? From an African and continental perspective, what features would one hope to see in the domestication of data/cloud policy? To what degree are the rationales and concepts within these policy domains and these processes of formulation and domestication rights-preserving? Do they go far enough in promoting data justice? From an economic point of view, what do these policies mean for industries concerned with the digital economy and for competition, innovation, and sustainability more widely?

ENDNOTES

1 Malcolm Kijirah and Elaine Wangari Thuo, 'Data Protection and Data Localization in Kenya: Potential Economic Impact and Effect on Kenya's Commitments in Various Regional Treaty Frameworks,' May 2021; Shanelle van den Berg, 'Data Protection in South Africa: The Potential Impact of Data Localisation on South Africa's Project of Sustainable Development,' June 2021; Lukman Adebisi Abdulrauf and Oyeniyi Abe, 'The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations,' June 2021.

2 Jonathan Klaaren, 'The Emergence of Regulatory Capitalism in Africa,' *Economy and Society* 50, no. 1 (January 2, 2021): 106, https://doi.org/10.1080/03085147.2021.1841934.

3 Firoz Cachalia and Alex Beyleveld, 'Exploring Legal and Policy Options to Address the Competition Inequality Nexus: The Case of South Africa,' in *UNCTAD Conference*, 2021, 36.

4 Graham Greenleaf and Bertil Cottier, 'Comparing African Data Privacy Laws: International, African and Regional Commitments,' April 22, 2020, https://papers.ssrn.com/abstract=3582478.

5 Greenleaf and Cottier, 'Comparing African Data Privacy Laws: International, African and Regional Commitments'.

6 Kashish Makkar and Saarthak Jain, 'Data-Related Abuse of Dominance in Digital Economy: A Template for Future Regulation in India,' July 15, 2020, https://doi.org/10.2139/ssrn.3652593.

7 'Online Platforms and Digital Advertising: Market Study Interim Report' (Competition and Markets Authority, 2019), https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf.

8 Marco Botta and Klaus Wiedemann, 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*,' *The Antitrust Bulletin* 64, no. 3 (September 1, 2019): 428–46, https://doi.org/10.1177/0003603X19863590.

9 Caron Beaton-Wells, 'Ten Things to Know about the ACCC's Digital Platforms Inquiry,' 2019, 17.

10 'The Data Portability Act: More User Control, More Competition,' New America, accessed March 7, 2020, https://www.newamerica.org/oti/blog/data-portability-act-more-user-control-more-competition/.

11 'Data Transfer Project Overview and Fundamentals,' July 20, 2020, https://datatransferproject.dev/dtp-overview.pdf.

12 GDPR Article 20:

> *(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); (b) and the processing is carried out by automated means. (2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. (3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. 2. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (4) The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.*

13 Akiva Miller, 'Is the California Consumer Privacy Act the Answer to Price Discrimination?,' SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, September 6, 2018), https://papers.ssrn.com/abstract=3245548; Graham Greenleaf and Bertil Cottier, 'Data Privacy Laws and Bills: Growth in Africa, GDPR Influence,' SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, April 12, 2018), https://papers.ssrn.com/abstract=3212713.

14 Martin Tisne, 'It's Time for a Bill of Data Rights,' *MIT Technology Review*, accessed March 11, 2020, https://www.technologyreview.com/s/612588/its-time-for-a-bill-of-data-rights/.

15 Katy Murphy, 'Wild West: Firms Interpret California's Privacy Law as They See Fit,' Politico PRO, accessed January 12, 2020, https://politi.co/2sR2jhw.

16 Beaton-Wells, 'Ten Things To Know About The ACCC's Digital Platforms Inquiry'; Graham Greenleaf, 'Australia Debates Tougher Privacy Regulation of Digital Platforms,' SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, September 18, 2019), https://papers.ssrn.com/abstract=3502659.

17 Caron Beaton-Wells, 'Platform Power and Privacy Protection: A Case for Policy Innovation,' *Competition Policy International*, 2018, 10.

18 Beaton-Wells, 'Platform Power and Privacy Protection: A Case for Policy Innovation'.

19 Mark Burdon and Tom Mackie, 'Australia's Consumer Data Right and the Uncertain Role of Information Privacy Law,' *International Data Privacy Law* 10, no. 3 (August 1, 2020): 222–35, https://doi.org/10.1093/idpl/ipaa008.

20 Burdon and Mackie, 'Australia's Consumer Data Right and the Uncertain Role of Information Privacy Law'.

21 Burdon and Mackie, 'Australia's Consumer Data Right and the Uncertain Role of Information Privacy Law'.

22 The next version of this policy brief can include material from the country briefs in this section.
23 Klaaren, 'The Emergence of Regulatory Capitalism in Africa'; Eleanor M Fox and Mor Bakhoum, *Making Markets Work for Africa: Markets, Development, and Competition Law in Sub-Saharan Africa* (Oxford University Press, 2019).
24 Ewan Sutherland, 'Digital Privacy in Africa Cybersecurity, Data Protection & Surveillance,' *SSRN Electronic Journal*, 2018, https://doi.org/10.2139/ssrn.3201310.
25 Klaaren, 'The Emergence of Regulatory Capitalism in Africa'.
26 Ministry of Information, Communication, Technology, Innovation, and Youth Affairs, 'Digital Economy Strategy (Kenya),' July 2020, https://ict.go.ke/wp-content/uploads/2020/08/10TH-JULY-FINAL-COPY-DIGITAL-ECONOMY-STRATEGY-DRAFT-ONE.pdf.
27 Competition Commission, 'Competition in the Digital Economy (Version 1),' (Competition Commission, September 7, 2020), http://www.compcom.co.za/wp-content/uploads/2020/09/Competition-in-the-digital-economy_7-September-2020.pdf.
28 Competition Commission, 15.
29 Ministry of Information, Communication, Technology, Innovation, and Youth Affairs, 'Digital Economy Strategy (Kenya),' 6.
30 Competition Commission, 'Competition in the Digital Economy (Version 1),' 10.
31 Competition Commission, 'Competition in the Digital Economy (Version 1),' 42.
32 Competition Commission, 'Data Services Market Inquiry: Final Report: Summary of Findings and Recommendations,' December 2019, http://www.compcom.co.za/wp-content/uploads/2019/12/Data-Market-Inquiry-SUMMARY.pdf.
33 Jason Bell et al., 'Structural Transformation in South Africa: Moving towards a Smart, Open Economy for All,' April 2018, https://static1.squarespace.com/static/52246331e4b0a46e5f1b8ce5/t/5ad9e4baf950b767531fe8a9/1524229357942/IDTT+Structural+Transformation+in+South+Africa+Moving+towards+a+smart%2C+open+economy+for+all.pdf.
34 The concept of sovereignty in the digital age raises a host of interesting and significant issues, some of them directly related to monetary sovereignty. Katharina Pistor, 'Statehood in the Digital Age,' *Constellations* 27, no. 1 (2020): 3–18, https://doi.org/10.1111/1467-8675.12475.
35 'The Digital Transformation Strategy for Africa (2020-2030),' accessed May 5, 2021, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.
36 'The Digital Transformation Strategy for Africa (2020-2030)'.
37 'The Digital Transformation Strategy for Africa (2020-2030)'.
38 Abdulrauf and Abe, 'The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations'.
39 Abdulrauf and Abe, 'The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations'.
40 'Guidelines for Nigerian Content Development,' Guideline 12.2(1).
41 'Guidelines for Nigerian Content Development,' Guideline 13.1(2).
42 'Guidelines for Nigerian Content Development,' Guideline 13.2 (3).
43 Abdulrauf and Abe, 'The (Potential) Economic Impact of Data Localisation Policies on Nigeria's Regional Trade Obligations'.
44 Kijirah and Thuo, 'Data Protection and Data Localization in Kenya: Potential Economic Impact and Effect on Kenya's Commitments in Various Regional Treaty Frameworks'.
45 Kijirah and Thuo, 'Data Protection and Data Localization in Kenya: Potential Economic Impact and Effect on Kenya's Commitments in Various Regional Treaty Frameworks,' 17.
46 Alex B Makulilo and Patricia Boshe, 'Data Protection in Kenya,' in *African Data Privacy Laws*, ed. Alex B Makulilo, Law, Governance and Technology Series (Cham: Springer International Publishing, 2016), 317–35, https://doi.org/10.1007/978-3-319-47317-8_15.ed. Alex B. Makulilo, Law, Governance and Technology Series (Cham: Springer International Publishing, 2016.
47 Makulilo and Boshe, 'Data Protection in Kenya,' 333.since Kenya has not yet adopted a specific data protection legislation, particular focus in this chapter is given to the data protection reform process. An assessment of the Data Protection Bill 2013 is central in this chapter. Also a discussion in this chapter will focus on the current case law decided by Kenyan courts based on the privacy protection afforded in the Kenyan Constitutions (the old and new
48 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy,' April 1, 2021, https://www.gov.za/sites/default/files/gcis_document/202104/44411gon309.pdf.
49 It may well be worthwhile to research and reflect upon the digital practice of inviting and disclosing comments and submissions as part of digitally enabled public-participation processes. Two empirical examples are this policy process and the one on the public-procurement legislation led by the OCPO.
50 Andrew Rens et al., 'ResearchICT Africa Written Submission in Response to the Proposed National Data and Cloud Policy' (ResearchICT Africa, June 1, 2021), https://researchictafrica.net/wp/wp-content/uploads/2021/06/RIA_Submission_DATA_and_Cloud_Policy.pdf.
51 'South Africa: New Draft National Data and Cloud Policy,' *Bowmans* (blog), accessed April, 19, 2021, https://www.bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-new-draft-national-data-and-cloud-policy/.
52 Jonathan Klaaren, 'The South African "Secrecy Act": Democracy Put to the Test,' *Verfassung Und Recht in Übersee VRÜ* 48 (2015): 284–303.
53 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy,' 25.

54 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy,' 32; Musoni Melody, 'Is Cyber Search and Seizure under the Cybercrimes and Cybersecurity Bill Consistent with the Protection of Personal Information Act?,' *Obiter* 37, no. 3 (December 1, 2016): 683–94, https://doi.org/10.10520/EJC-7e4a98eea.

55 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy,' 31–34.

56 Jan Vermeulen, 'South Africa's Plan to Launch State-Owned Cloud Computing Mega-Network,' accessed April 12, 2021, https://mybroadband.co.za/news/cloud-hosting/392105-south-africas-plan-to-launch-stated-owned-cloud-computing-mega-network.html.

57 'Data Generated in SA Is the Property of SA, Says New Draft Govt Policy – and Cops Need Access,' BusinessInsider, accessed April 12, 2021, https://www.businessinsider.co.za/a-draft-national-data-and-cloud-policy-demands-data-sovereignty-for-south-africa-2021-4.

58 Tim Cohen, 'Critics of SA Government's Proposed Digital Grab Idea Express Deep Concerns,' *Daily Maverick*, May 3, 2021, https://www.dailymaverick.co.za/article/2021-05-03-critics-of-sa-governments-proposed-digital-grab-idea-express-deep-concerns/.

59 Anthony Butler, 'Getting off the Ground,' Practical Reason (blog), April 2, 2021, https://practicalreason.blog/2021/04/02/getting-off-the-ground/.

60 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy,' 12.

61 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy,' 34.

62 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy,' 25.

63 'Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy,' 30.

64 Van den Berg, 'Data Protection in South Africa: The Potential Impact of Data Localisation on South Africa's Project of Sustainable Development,' Rens et al., 'ResearchICT Africa Written Submission in Response to the Proposed National Data and Cloud Policy.'

65 Industrial Development Think Tank, 'Towards a Digital Industrial Policy for South Africa: A Review of the Issues' (CCRED, July 17, 2019), https://static1.squarespace.com/static/52246331e4b0a46e5f1b8ce5/t/5d355997ae8bf40001ee2906/1563777435535/DPIP_Final.pdf; Industrial Development Think Tank, 'Policy Proposals for South Africa on the Digital Economy,' Policy Brief (CCRED, May 2020).

66 Industrial Development Think Tank, 'Policy Proposals for South Africa on the Digital Economy'.

POLICY BRIEF 05

MANDELA INSTITUTE

ABOUT THE MANDELA INSTITUTE

The Mandela Institute is a centre in the School of Law of the University of the Witwatersrand. The Mandela Institute conducts research, develops policy and offers basic and advanced teaching in different areas of law. Further, the Institute conducts executive teaching, training and capacity-building through offering short-course certificate programmes, conferences, and public seminars in areas of law and policy which are domestic in operation but are impacted by global developments.

ABOUT THIS POLICY BRIEF

This Brief is part of a series of publications under the Mandela Institute's 2021 research project on The Economic Impact of Data Localisation in Africa. This project is funded by Facebook.

ABOUT THE AUTHOR

Jonathan Klaaren is a Professor at the University of the Witwatersrand in Johannesburg, South Africa, serving at the Wits Law School and with the Wits Institute for Social and Economic Research (WiSER). He is a former dean of the law school as well as former director of the Mandela Institute.

Mandela Institute, School of Law
School of Law Building
Braamfontein West Campus
University of the Witwatersrand
Johannesburg 2000
South Africa

www.wits.ac.za/mandelainstitute

Design and layout by COMPRESS.dsl | 400427 | www.compressdsl.com