
RESEARCH
ICT AFRICA

Written submission in response to the:

PROPOSED NATIONAL DATA AND CLOUD POLICY

as published by the Minister of Communications and Digital Technologies in terms of Section 3 (5) of the Electronic Communications Act 2005 in Government Gazette No. 44389 of 1 April 2021.

Ms C Lesufi, Director, Telecommunication Policy
DataCloudpolicy@dtps.gov.za

1 June 2021

For further information please contact:
Dr. Andrew Rens, Senior Associate,
Research ICT Africa

arens@researchictafrica.net

About Research ICT Africa

Research ICT Africa (RIA) is a regional digital policy and regulation think tank based in Cape Town and active across Africa and the global South. It conducts research on digital economy and society that facilitates evidence-based and informed policymaking for improved access, use and application of information and communication technologies (ICTs) for social development and economic growth. RIA also has a dedicated digital policy unit which specialises in Internet governance, digital rights, cybersecurity, gender, innovation (including artificial intelligence and the Internet of Things), and data justice. Understanding the needs and digital challenges of marginalised communities – including women, youth, children, the elderly, and people in rural areas, for example – form an integral part of RIA's work.

Acknowledgements and declaration

This submission was drafted and prepared by Gabriella Razzano, Anri van der Spuy, Kristophina Shilongo, and Andrew Rens, with valuable inputs, contributions and revisions from other RIA staff members. It includes contributions by Professor Jonathan Klaaren of the Wits Institute for Social and Economic Research. Any errors or omissions remain the authors' own.

The research informing this submission is funded by a grant from Canada's International Development Research Centre (IDRC) to develop cyberpolicy capacity in Africa

Availability

We confirm our availability to make oral representations based on this submission should public hearings be held.

Overview

Research ICT Africa (RIA) welcomes this opportunity to submit written comments in response to the Proposed National Data and Cloud Policy, published by the Minister of Communications and Digital Technologies in the Government Gazette in April 2021.

We make this public interest submission to help ensure that the intensifying global processes of digitalisation and datafication can be harnessed to contribute to the national project of reducing poverty, unemployment and inequality and ensuring that the benefits of advanced technologies and opportunities to innovate, improve lives and livelihoods are more evenly spread. We acknowledge the work done by the Ministry and the Department of Communications and Digital Technologies in developing the draft cloud and data policy in order 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 and welcome the opportunity for further input from stakeholders.

Research ICT Africa shares many of the same goals as the policy, not least ensuring that the socio-economic benefits of data and cloud computing are shared by all living in South Africa. Our extensive work on telecommunications and digital policy over the past fifteen years across Africa compels us to ensure more positive and equitable policy outcomes, guarding against the growth in digital inequality that is being experienced as the processes of digitalisation and datafication intensify. This is not only in the form of the traditional digital divide between those connected and those not connected by also between those barely connected on low value data bundled passively consuming essential services and those who are actively gathering information, reducing their costs by transacting online and generally able to improve their lives or even productively contributing to the prosperity of their nations.

This submission is made in the knowledge that these inequalities reflect the structural inequalities that characterise our economy and the need in policy formulation to actively redress historical injustices reflected in inequality today.

This needs to be done in a way that acknowledges the resource constraints within the state and leverages the resources in the private sector and civil society. Fundamentally, in its broader approach it needs to balance demand-side valuation with the prevailing commercial supply-side valuation used for the allocation of resources in policy and regulation over the past four decades globally. Three key policy insights emerge from this demand-side, value-creation-focused analysis. First, digital infrastructure resources are fundamental resources that generate value when used as in-puts into a wide range of productive processes. Second, the outputs from these processes are often public and non-market goods that generate positive externalities that benefit society. Third, managing infrastructure resources in an openly accessible manner may be socially desirable when it facilitates these downstream activities. (Frischmann, 2004). The importance of public and social value generated by digital infrastructure investments in addition to the more obvious appropriable rents of commercial models, have been highlighted by the pandemic and the associated lockdowns.

Evidence shows that while the online economy surged in growth and mobile data services boomed with exponential demand for bandwidth only a relative elite were able to move seamlessly online and digitally substitute their banking, food provision, schooling and office work and even access business or unemployment relief or safely receive their social grants. For the majority of those who own an Internet enabled device, while depending on tiny, small value data bundles, significant digital substitution such as remote work or schooling is as unfeasible as not being connected, which is still the case for more than 40 percent of South Africans. The pandemic and lockdown and the inequitable access to digital services have had a compounding effect on existing structural inequalities. As indicated above digital inequality has long been known to reflect underlying structural inequalities affecting life opportunities in contemporary society but the pandemic has threatened those without meaningful access' very survival.

The importance of prioritising these issues in the data and cloud policy in the preparation of the country for the next inevitable pandemic and for post-COVID economic reconstruction, particularly in the context of the African Continental Free Trade Area becoming operational, is clear in President Ramphosa's

recognition of digital inclusion being central to a new more just social contract. Its finalisation also needs to be considered in the context of calls by the UN Secretary General, Antonio Guterres, to ensure that greater progress is made to meet the digital targets underpinning several of the 2030 Sustainable Development Goals, to ensure that the digital revolution does not widen inequalities even further (Guterres, 2020).

In countries like South Africa, where only about 53% of the population was online in 2018 (Gillwald et al., 2018), it is essential that any policy guiding technological developments ensure greater access and take into account the interests of those not online. It is therefore important to keep in mind that in South Africa, significant access discrepancies persist between rural or urban areas, between women and men, between poor or wealthier segments, between literate or illiterate people, and between children, adults and the elderly. For those who are online, Internet use is often intermittent and passive. A relatively small number of South Africans actually have the skills or resources to participate meaningfully online (Gillwald et al., 2018) - or to protect themselves from the risks that accompany digital inclusion. As access to the Internet increases in our country, users are exposed to new or different threats and risks in addition to the ones they face 'offline' in particular in respect of privacy.

As the Internet and digital inclusion increasingly becomes a precondition for participation in today's society – from the provision of e-government services like access to an identity document to procuring social benefits, performing work, accessing finance, or gaining education – it is critical that all South Africans are able to use various ICTs. The Internet and 4IR should be a space which enables users to exercise their rights.

General comments and concerns

With this background in mind, and before submitting comments on specific aspects of the *Proposed National Data and Cloud Policy*, we highlight the following overarching concerns or considerations before delving into specific provisions of the proposed policy:

- Framing data as infrastructure seems to have led to the questionable claim that data can be owned in the legal sense and that realising value from data is achieved through excludability, rather than through processing and transfer.

  The Policy should frame data as creating value through real time data flows and confluence rather than as static, exclusively controlled databases.

- There are three problematic assumptions that underlie the protectionist approaches to data solutions: the first, as mentioned it above, is a belief that because data is valuable in the digital economy its value is best extracted from seeking excludability; the second, is that data infrastructure and data needs can be conflated; and the third is that personal data necessities align with *all* data necessities.

  The Policy should start with a more detailed consideration of data, data types and data value, as informed by international discussions in the area.

- While there are risks to cross border data flows, the proposed policy focuses on the risks rather than the opportunities in terms of data portability and as a result takes a protectionist approach.

  The Policy should set out how opportunities to attract data hosting and data processing investments and data flows into South Africa, especially through the developing African Continental Free Trade Agreement as well as from the European Union and more strongly requiring data portability.

- Data and cloud policy fall within the remit of the Minister and the Department. However the proposed policy is wide ranging and cross cutting raising concerns regarding the Departments capabilities to implement and enforce such a cross-cutting policy. Is this within the remit of the Department? Both the Information Regulator and the Competition Commission play key roles in the digital economy, coordination with them is vital.

  The Policy should require both continual recognition - and coordination - with both the Competition Commission and Information Regulator of South

Africa.

- Given the immense centrality of skills and capacity in reaping digital dividends, a larger focus should be placed on considering the enabling environment necessary for building such skills within the policy, but also - given the public sector data focus - enhancing the public sector capacities in data skills, inclusive of personal data protection.
  The Policy's approach to data skills should reflect existing digital inequalities compounded by the new digital skills divide owed to a shortage in data science and analytics. In particular the Policy should commit to increase funding for data intensive research in universities to develop not only skills but the capacity to generate more skills.

- There is a significant underrepresentation of the government's efforts to pursue data justice, through cross-sectoral collaboration (civil society, intergovernmental, international), ensuring ethical data practice and equitable use/access to data
  The Policy should detail how the Advisory Council for Data Practices could operate as a possible form of multi-stakeholder participation within data governance, informed by social and economic perspectives and expertise.

- The Open Data imperatives articulated in the Policy are incredibly important as they address a significant gap in policy frameworks and extend international commitments made under the Open Government Partnership.
  The National Open Data Strategy should be the first priority.

- The proposed policy makes important points: the need to support local innovation communities; the need for public data practices and capacities to be a priority is vital; and the central role that open data ecosystems (and underlying data structure norms) play in deriving digital benefits, however these insights are not well reflected in the policy recommendations. The policy should take into account how data localisation, and the practical efforts that would be required for data localisation, would directly lead to increased burdens on local innovation

communities.

The Policy should make recommendations how innovation communities may be fostered. The policy should also specifically engage with possibilities for regulatory sandboxes on different data issues that could facilitate local development.

Specific comments on the nature and value of data

Much of our above recommendations, and later commentaries, are based on a particular understanding of the nature and value of data. It is thus worth preceding the rest of the document with an introduction to this understanding.

Data, generally, is non-rivalrous (at the technical level, it is infinitely usable without detracting from another person's ability to use it) (Jones & Tonetti, 2020). Yet as far as excludability is concerned, the law (through both claims of copyright and contract) is often used to drive the economic value of data from outside the bounds of a "public good" and defines it through partial excludability (Carrière-Swallow & Haksar, 2019). Supposed ownership of data through legal excludability is often complicated by attempts to frame control of personal data as a species of ownership rather than autonomy, control and public concern. It is the collective nature of data collection (and the ability to store it and analyse it collectively) that in turn actually drives economic value for firms – big data is the source of the anti-competitive dominance of the GAFAM (Google (Alphabet), Apple, Facebook, Amazon, and Microsoft) and BATX (Baidu, Alibaba, Tencent, Xiaomi) companies (Thieulin, 2019), alongside the capacity to interpret that data, but also (to a degree) to sell it on (Noble, n.d.). Yet the reality is data brokerage is increasingly only secondary to the economic value that the dominating firms can extract from interpreting that data and feeding it into their own product and service design, which relates to economies of scale (Martinez, 2019; Mitretodis & Euper, 2019).

Statements like "data is the new oil" contribute significantly to blurring the lines which define the economic value of data, and the underlying incentives that might inform - or impede - its governance. The idea that simply gathering more and more data creates economic benefits for companies actually does not recognise the microeconomic realities of data (Casado & Lauten, 2019), yet has

significantly driven data practices (there are however economies of scale in terms of the data collection costs for companies (Carrière-Swallow & Haksar, 2019)). This is because network effects related to data are not the same as data network effects, and in fact data is more often connected to scale effects for business, that can be overstated (Casado & Lauten, 2019). Complexities are born of trying to determine the value of data outside of the technologies they drive, and in considering the value of data as a factor of production (Carrière-Swallow & Haksar, 2019). However the other component of value from data is generated when data is used to create information, and shifts this information across agents. This ability of data to increase efficient economic transactions directly implicates how much of the value of data can be derived from its "flow" (Carrière-Swallow & Haksar, 2019). It is also important to consider amongst other criteria, that macroeconomic benefits of data are also derived from this flow (e.g. market efficiencies and competition from reduced information asymmetries) (Carrière-Swallow & Haksar, 2019).

Specific comments and concerns

Besides these general comments, we now respectfully submit comments in response to specific headings of the policy:

Response re: Background and Context

There are important acknowledgments within the description of background and contexts worth highlighting. Certainly, a focus on *infrastructure* is vital for reaping digital dividends - and this implicates the need for direct public investment, including into Cloud infrastructure. Concurrently, it highlights the need to support local innovation communities to drive local development and benefits.

The importance of public data practices being improved is central - which includes improving both human and infrastructure capacities for the public sector (tied to open government imperatives). Open data and open systems are acknowledged as central to deriving benefits for both the public and private sector. Yet, these important acknowledgements and sections don't necessarily

resonate strongly in the policy recommendations.

Response re: Policy, Legislative and Regulatory Landscape

The proposed policy seeks to provide an 'ideal policy and regulatory environment' to support and drive the development of the digital economy. This aim would be closer to realization if supporting policies, legislature and the general regulatory landscape adjacent to this policy were thoroughly reviewed for constitutionality and updated.

Reference to the Protection of Personal Information Act and Minimum Information Security Standards is appropriate but should acknowledge their significant inadequacies, and should not then centre them as instructive for the policy. This is because the Protection of Personal Information Act is currently under review. And the Standards have not been created through a public participation process and have long been recognized as suffering from constitutional infirmities (Klaaren, 2002). Further, the policy occupies in part the policy space on the classification of information held by the state, a space still taken up by the Protection of State Information Act, a piece of legislation approved by Parliament, subject to strenuous constitutional objections and two) Presidential referrals, and currently within Parliament's jurisdiction once again. The policy presumes the validity of that now by-passed piece of legislation and proposes in policy intervention 10.3.5 that "[t]he Protection of State Information Legislation shall be reviewed, where necessary, to enable protection of sensitive data in the digital economy." The review of that draft legislation should go much further. Finally, the policy should incorporate adjacent policies which may not be data related and, although they cannot be regulated by this policy, are integral to the data ecosystem, such as those relating to Education, Taxation, Trade, Infrastructure and Competition.

The proposed policy deals with research data produced by universities and science councils; research data is at least partially affected by the Intellectual Property from Publicly Funded Research Act which prohibits universities from making it open data as suggested in the policy, and would prohibit giving data to the (central database) without incurring extensive administrative burdens of obtaining permissions. An obvious solution would be to amend the Act to exclude

research data from its definition of intellectual property, a definition that already excludes scholarly publications. This would seem a relatively minor amendment.

The extent to which data and databases are subject to intellectual property, in particular copyright, is unclear, but this lack of clarity is at least partially resolved by the Copyright Amendment Bill 2018 which is currently before Parliament. However copyright does not apply to a particular datum (data point), nor to data flow and likely does not apply to computer generated data without an ascertainable human author. The Copyright Amendment Bill clarifies the extent to which compilations of data are subject to copyright in section 2A. Passing the CAB would address the lack of clarity about copyright in data*bases*. However copyright in data*bases*, although not in data nevertheless creates challenges for researchers, and an exception to copyright in databases is required to permit such research. The CAB includes an exception (section 12A) that would enable research. Passing the CAB and would be a quick and relatively easy policy action.

Response re: Rationale for the Data and Cloud Policy

The economic and development reasoning behind the proposed policy are clear, however given the pre-existing structural inequalities which have led to a wide digital divide – the policy should factor in a data justice approach. It is silent in addressing the societal implications of datafication, which implicates not only data subject rights very directly, but also should seek to facilitate direct citizen participation in data management and oversight. These gaps often occur in policies related to data that prioritise its economic role, over its broader relevance to both social outcomes, and political participation. The rationale also rests on a dated view of data, and how value may be obtained from data, addressed above.

Response re: Global Trends

Given the global ramifications of data management and exchange, there is a gap: the proposed policy's inability to establish preliminary policy positions for engaging in the international and regional, political and multi stakeholder governance forums of relevance to the data ecosystem, such as the African Union Commission, World Trade Organisation, Internet Governance Forum,

ICANN, etc. The proposed policy, which later criticises difficulties in engaging dominant foreign technology companies, is notably lacking in an engagement with the global political forums seeking to constrain, or at least engage with, questions of economic and political power dimensions of data and data control. The Policy should make clear the political position for engaging in such forums actively as a productive step for dealing with some of the challenges identified.

Response re: Purpose

The purpose of the Policy should include reference to desirability of enabling data transfer to South Africa.

Response re: Scope

The scope should include South Africa's relationship to other countries and jurisdictions.

Response re: Vision

The vision is articulated in a technocentric way rather than envisioning how the government and South Africa might best benefit, both socially and economically.

Response re: Objectives

The objectives should include the following:

- Enabling South African enterprises including SME's to process data from other countries efficiently and with appropriate safeguards.
- Support participation in the African Continental Free Trade Agreement.

Response re: Definitions

It would be helpful if the Policy would specify which categories of data the policy is referring to and what type of information will be generated from it. The policy would benefit from clear descriptions of at least some of the important categories of data such as personal data, financial data, scientific data and metadata. These are classifications in terms of *function* which has a strong influence in helping to determine the justifiability of limitations posed on data forms. As detailed by

Helen Nissenbaum (Nissenbaum, 2009), protections should reflect the manner and purpose for which data is processed. While the proposed policy fails to engage fully with functional definitions in data, it also creates additional definitions out of keeping with the definition in the two key information regimes for South Africa: POPIA and PAIA. So for instance, ‘sensitive data’ is not a form of definition that arises from either law. Nor does it in fact even arise from the MISS, which discusses data as being that data which is classified across certain streams - classifications that aren’t included in the proposed policy.

Response re: Policy Intent

The Policy intent should emphasise the importance of digital trust. A large portion of the population have no or limited experience of data intensive environments. Establishing digital trust is an important aspect of inclusion. Before people are willing to entrust their data to 3rd parties, trustworthy structures and processes must be put in place.

Response re: Policy interventions

a. Policy Issues on Digital Infrastructure

The Policy should quantify how much power and bandwidth capacity to support critical infrastructure for data will be needed, especially to incorporate next wave technologies such as Artificial Intelligence and Internet of Things.

The Policy should address how education, specifically higher education will address the projected demand for data centre technicians needed for data centres. There is a need for technical capacity simply to run data centres, the need for data analytic capacity should be addressed under Capacity.

The recommendation in 10.1.8. that “data centres may make provision for self-generation energy capabilities” is strongly supported in the context of commitment to green energy. However to encourage investment in self-generation capabilities it must guarantee that there will be no maximum limit on self generation capacity.

The policy should specify how exactly special economic zones (SEZ) woul be introduced, and could be successful, and in particular what specific policies would attract investment and enterprises to these zones. The policy should address how the increased demand created by data centres not only for bandwidth and electrical energy but for water for cooling purposes may be addressed in SEZs. The Policy should consider measures that would encourage establishment of data centres in SEZs for example licensing data centres to onsell bandwidth to geographically adjacent enterprises. Physically adjacent enterprises could connect to neighbours to pool bandwidth without using other networks. Data centres that self-provide energy in SEZs should be permitted to onsell energy to physically adjacent neighbours if they can do so without recourse to the national grid.

b. Policy issues on Access to Data and Cloud Services

The policy also needs to place significant attention on creating the parameters for open (and other) data standards that can practically facilitate interoperability and sharing across departments, spheres and institutions (Razzano, 2016). The development of a National Open Data Strategy is both urgent and important and should be prioritised. However, centering the political champion for the open data strategy should also directly acknowledge the potential role of the Information Regulator of South Africa.

In developing the National Open Data Strategy the terms on which data is shared must be uniform across government. To facilitate this a rigorous definition of open data must be used. The most coherent and internationally recognised definition of Open Data is offered by the Open Definition (https://opendefinition.org/). To prevent data being siloed by legal terms the National Data Strategy should mandate a single, internationally recognised license for using data. If different levels and branches of government develop their own terms, the terms will be incompatible and the data may not be combined. If the terms used by the government, even if uniform across government, are incompatible with data sets under internationally recognised terms, then researchers and South African enterprises will have difficulty combining the datasets. Therefore the strategy should mandate the

internationally recognised Creative Commons Zero (https://creativecommons.org/share-your-work/public-domain/cc0/) terms for open data.

Recommendation 10.2.4 supports the establishment of frameworks for data trusts. Although these may operate in ways similar to trusts they should be overseen by an expert regulator such as the Information Regulator, and not by the office of the Master of the High Court, which lacks digital capability. More fundamentally the creation of data trusts is not yet reconcilable with South African law given the requirement that trusts hold property, and also given the challenges in determining *identifiable* data (remembering for instance that assured lineage in data can only be achieved through the utilisation of non-fungible tokens), though the remit in relation to personal data would be more realistic. There are forms of stewardship that might get around these legal challenges, but the Policy will need to engage definitively in the complex legal debate that underlies data, ownership, and property (as addressed in part in the discussion on data ownership).

c. Issues on Data Protection- Issues

The centralisation of POPIA and emerging data protection norms in South Africa are important. The policy would be enhanced however by clarifying its approach to data portability issues, given the lacuna in current governance frameworks post-POPIA.

Perhaps focusing more on data protection policy than competition policy, the proposed 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.” However the only non-sourced use of the concept comes in the presentation of policy interventions flowing from the engagement with competition questions. 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. A broader and more coordinated policy in respect of portability across government is called for. Policy on data portability is under discussion within the market enquiry currently being conducted by the Competition Commission.

Importantly, the holding of public sector data on the HPDCD Cloud for ‘sensitive’ data will have to -as the Policy acknowledges - be able to facilitate the Promotion of Access to information Act, and its obligations and requirements, within its system and requirements.

d. Policy issues on Localization and Cross Border Data Transfers- Issues

On Co-ownership of Data

The state’s role in the function of managing data stored at the Digital Transformation Centre or how it will coordinate its management should be made more clear than currently stated, as well as the economic advantage of such a practice. The policy argues that the South African government is thus compelled to play "a more central role in the collection, dissemination, and analysis of data, understanding that key economic advantages are contained within it." It further states that while the government supports the free flow of information and information as articulated in POPIA, it deems the protection of citizen data as central to participation in the global digital economy.

The assertion of the state as a co-owner of data is problematic and should be abandoned, or at least far more clearly delineated. The problem with the notion of ownership of data is not only its inconsistency with how value is *actually* extracted from data (as addressed earlier, the value of data is extracted through control not ownership). There are also significant problems in relation to the basis of any claim of ‘co-ownership’ in law. In law ownership is based on a ‘thing’ that can be owned. What is the ‘thing’ under discussion here? Much of the Policy actually seems based on notions of static data in databases, access to which is excluded for all but a few or one actor - whereas the value of 'the Cloud' is the provision of real time data access for businesses and consumers. Much data is generated from products continuously, in a non-rivalrous manner. This also raises

questions as to when the ‘thing’ is generated ‘in South Africa’ - much metadata is generated at the server itself - data is a chain, rather than a point. Its nature means that defining the ‘thing’ authentically is practically impossible, hence references to ‘partial’ excludability.

The policy fails to establish the *legal* basis for such co-ownership. The challenge for legal ownership is acknowledged in the paper which itself states the lack of clarity of Intellectual Property especially Copyright on data. Other than Intellectual property on what legal basis could such ownership be based? As previously stated the Copyright Amendment Bill will clarify copyright law in line with international developments. In keeping with those developments copyright will only cover data*bases* and not data. Copyright will not cover all databases, but only those that by reason of their selection or arrangement of their content are original works. Furthermore, to be the subject of copyright a database must have a human author: many computer generated databases may not be under copyright. Copyright explicitly does not extend to an individual datum (data point), thus data extracted from a copyright protected database may be freely used. Although the phrase ‘Intellectual Property’ includes the word ‘property’ Intellectual Property is not regarded as property in South African law but is instead treated as a separate system. Whether any type of intellectual property is property for the purposes of section 25 of the Bill of Rights has not been decided by the Constitutional Court, however to the extent that copyright in databases is property for the purposes of the Bill of Rights that undercuts the notion of state co-ownership.

Assertions of ownership of data thus have no clear legal basis. But even if ownership in data is possible no basis for co-ownership is established. While a policy may suggest an intention to establish a legal basis for co-ownership that is not sufficient to change the law. The policy does not fully grapple with the implications of asserting that data is capable of ownership, since if data may indeed be owned then it likely constitutes property for the purposes of Section 25 of the Bill of Rights and, if so, the state may not arbitrarily deprive any person of their rights to that property. But of course, the nature of data and its non-rivalry mean that creating ‘standard’ ownership regimes other than through non-fungible tokens is not feasible.

Importantly, much of this discussion on data ownership also extends to data trust and trustee recommendations, addressed above, under the data protection recommendation. There is very important emerging discourse on data trusts and *other* forms of stewardship as mechanisms for enhancing data protection. Before the Policy can make recommendations about ownership it must address and resolve a central problem: current law only provides trustee rights over property.

However if the use of the words property and ownership are meant only to suggest that South Africa should exercise sovereignty over South African data and thus regulate how it is used including that economic benefit from South African data is derived by South Africa then speaking of ownership and property is confusing and unhelpful and sovereignty, control and benefit should be used instead.

On Data Localisation

While it is important for the policy to fit the local context, on some level it needs be synchronous with regional (SADC), continental (AUC) and global (BRICS, UNCTAD) agreements. In fact, throughout the Policy there is significant departure from existing multi-stakeholder forums of relevance to both data governance, and the digital economy.

The African Continental Free Trade Agreement (AfCFTA) represents a significant opportunity for South Africa's economy. However, benefiting from increased continental trade will require that South African businesses are able to move data originating in South Africa into other countries in the Free Trade area, and also to provide sufficient guarantees for the privacy of data from other countries. Without efficient data flow even non-digital trade will suffer. The European Union experience is instructive in this regard, the way to achieve efficient data flow is through a common data regulation. The policy should enable rather than prevent cross border data flows. The positions on sovereignty and localisation need to support data flows required for increased trade under the African Continental Free Trade Agreement (AfCFTA) and to enable South Africa to take a leading role in building the digital economy in Africa.

South Africa has a growing data processing industry including businesses that process data from the European Union in part due to sharing time zones with the European Union. Personal data originating in the European Union is subject to the General Data Protection Directive. Article 45 of the General Data Protection Regulation makes provision for the data protection standards in a country outside the union to be assessed as offering adequate protection for personal data originating in the union. An adequacy decision would greatly increase South Africa's competitiveness as a locale for data processing, and may become essential as other countries compete for data processing. However the policy does not acknowledge the importance of obtaining an adequacy decision nor commit to providing the kind of legal and policy environment necessary to obtaining an adequacy decision.

POPIA sets standards for personal data processing that support an adequacy decision. However the suggested policy on cross border transfers weakens the possibility of an adequacy decision as it is apparently inconsistent with the current cross-border provisions: it seemingly contradicts data minimalism requirements by requiring duplication of data, and potentially contravenes security provisions as decisions relating to where data is stored are mandated, rather than being based on decisions that reflect on adequate security safeguards of the storage facility selected). The Policy should clarify how the proposals that seem to be in conflict with POPIA can nevertheless comply with POPIA.

In respect of tax issues, the policy discussion on localization and the proposed policy do not engage with the data arguments, and provisional policy positions, developed on behalf of South Africa by the DTIC-funded Industrial Development Think Tank (Industrial Development Think Tank, 2020a, 2020b). This body of research has made two key proposals in respect of data localization 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, telecommunications; online search and location

data; and financial and transactions data)(Industrial Development Think Tank, 2020a). As can be seen, that second recommendation connects to our flags in relation to both definitions, but also the importance of centring the *functions* of data within a digital economy and social democracy.

On Research Data

In policy recommendation 10.4.4. the draft policy states that “All research data shall be governed by the Research Big Data Strategy of the Department of Science and Innovation (DSI).” However the Big Data Strategy is not publicly available. As result not only is the governance of research data unclear and the public excluded from commenting but the coordinating role of the Data and Cloud Policy is undercut.

e. Policy issues on Cybersecurity Measures

If the Digital Transformation Centre is a located at a single venue at which vast amounts of South African data are concentrated, which seems to be what is being proposed, that would present both an extremely attractive target for cyber attacks and cyber criminals and a single point of failure. The Policy should take this risk into account and explain why it is worthwhile rather than an approach in which government dataholders must maintain data in multiple interoperable datacentres from which data can be drawn together by the Digital Transformation Centre.

The Policy largely reconfirms current proposals on Cybersecurity. The National Cybersecurity Policy Framework (NCPF) and other related policies, legislation and international best practice are required to guide the implementation of initiatives and measures...

Yet, broad acknowledgments of the importance of cybersecurity are contradicted by requirements to duplicate storage on South African-based servers, regardless of the early emergence of cybersecurity standards and policies - with the Cybersecurity Bill not yet in place.

f. Policy issues on Governance and Institutional Mechanisms

The policy would benefit from clarity on the proposed mechanisms that will be in place to regulate the proposed Digital Transformation Centre, though the establishment of an Advisory Council on data management is an interesting suggestion. The Policy must outline how they plan to work alongside the Information Regulator, ICASA and the Competition Commission, and in fact whether creating new forms of governance and institutional mechanisms is even necessary - or if instead better coordination with existing Regulators, and institutions directly associated with implementation of policy, may be better recommendations accompanied by inclusion of new forms of multi stakeholder participation.

g. Policy issues on Competition

The policy identifies market concentration in the data and cloud computing market as giving rise to risks to competition and consumer choice. In addition to these risk concentration of personal data gives rise to another risk. A single corporation may control a significant percentage of a data market so that a data breach may affect millions of people. For example the Experian data breach exposed the private data of 24 million South Africans (*Experian Data Breach*, 2020). The danger is that the concentration of data by a few actors results in large scale failure that affects significant portions of the population even if conventional competition analysis does not identify an issue. The Competition Commission can already act to prevent mergers contrary to the public interest. However data concentration has not been acknowledged as a significant public interest. The policy should draw attention to mergers and acquisitions that enable the concentration of data of more than a significant percentage of the population. One approach would be to have parties involved in a merger demonstrate that they are not creating an increased risk of a large scale data breach.

Policy Action: The Policy should request the Competition Commission to consider the public interest in mergers and acquisitions that enable the parties to collect or control the personal data of a significant number or percentage of the population as creating a systemic risk.

Policy Action: The Policy should also ensure it is aligned with the Competition Commission's emerging work on "Competition in the Digital Economy".

h. Policy on Skills and Capacity Development

In addition to the need for the Policy to address how the increased demand for data centre technologists it should also deal with the increased demand for data analysts and data scientists. The discussion of the skills shortage should include the brain drain experienced in Africa due to data science skills shortages in the global north. Push factors such as the lack of research funding should be addressed. The policy should develop an approach to bridging the skills gap should factor in collaboration with academic institutions and businesses.

Policy Action: Address the lack of research funding for data intensive research.

i. Research, Innovation and Related Human Capital Development

Although the policy suggests that research access will be available to South African researchers to provide guidance to universities and research councils it should resolve the conflict with the Intellectual Property Rights from Publicly Financed Research and Development Act 2008. In terms of section 5 of that Act anything created by a university or research council that can be protected by intellectual property laws anywhere in the world must not be disclosed but must be commercialised. Since databases may be subject to ownership in the European Union in under the Database Directive somewhat absurdly South African universities may be deterred from making data openly available because the data in a database could theoretically be owned in another country even though it likely could not be in the Republic of South Africa. Universities may be wary of transferring data to a central database without the specific permission of the National Intellectual Property Management Office unless the law is clarified.

Policy Action: Amend the definition of intellectual property in Intellectual Property Rights from Publicly Financed Research and Development Act 2008 to exclude research data.

The draft policy stipulates that data must be "findable, accessible, interoperable and re-usable". The policy has also acknowledge that status of data in Intellectual Property is equivocal. While most data and uses of data may not be subject to

intellectual property laws several jurisdictions including the European Union and the United Kingdom have enacted ‘data mining’ exceptions, however these have been criticised as too narrow or difficult to use. The United States has not needed to enact a specific data mining exception since it can rely on fair use. South Africa could also rely on fair use since a fair use provision was included in the Copyright Amendment Act 2018. However for as long as the bill remains in parliament South African researchers face uncertainty that may deter them from data intensive research.

Policy Action: Pass the Copyright Amendment Act 2018 including the fair use provisions set out in Section 12A as a matter of priority.

References

Carrière-Swallow, Y., & Haksar, V. (2019). *The Economics and Implications of Data: An Integrated Perspective* (No. 19/16). https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

Casado, M., & Lauten, P. (2019, May 9). *The Empty Promise of Data Moats. Andreessen Horowitz. https://a16z.com/2019/05/09/data-network-effects-moats/*

Experian Data Breach. (2020). South African Banking Risk Information Centre. https://www.sabric.co.za/media-and-news/press-releases/experian-data-breach/

Frischmann, B. M. (2004). An Economic Theory of Infrastructure and Commons Management. *Minnesota Law Review*, *89*, 917.

Gillwald, A., Mothobi, O., & Rademan, B. (2018). *The State of ICT in South Africa* (After Access Policy Paper No. 5, Series 5; Policy Paper Series 5: After Access-Assessing Digital Inequality in Africa). Research ICT Africa.

https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf

Guterres, A. (2020). *United Nations Secretary-General António Guterres's Nelson Mandela Annual Lecture 2020*. Nelson Mandela Foundation. https://www.nelsonmandela.org/news/entry/annual-lecture-2020-secretary-general-guterress-full-speech

Industrial Development Think Tank. (2020a). *Policy Proposals for South Africa on the Digital Economy,* [Policy Brief]. CCRED.

Industrial Development Think Tank. (2020b). *Towards a Digital Industrial Policy for South Africa: A Review of the Issues*. CCRED. https://static1.squarespace.com/static/52246331e4b0a46e5f1b8ce5/t/5d355997ae8bf40001ee2906/1563777435535/DPIP_Final.pdf

Jones, C., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. *The American Economic Review*, *110*(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Klaaren, J. (2002). National Information Insecurity—Constitutional Issues Regarding the Protection and Disclosure of Information by Public Officials. *South African Law Journal*, *119*, 721–732.

Martinez, A. (2019, February 26). No, Data Is Not the New Oil. *Wired*. https://www.wired.com/story/no-data-is-not-the-new-oil/

Mitretodis, A., & Euper, B. (2019, July 29). *Interaction Between Privacy and Competition Law in a Digital Economy*. Competition Chronicle. https://www.competitionchronicle.com/2019/07/interaction-between-privacy-and-competition-law-in-a-digital-economy/

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (1st edition). Stanford Law Books.

Noble, J. (n.d.). *The murky world of data brokers | Financial Times*. Retrieved 3

September 2020, from https://www.ft.com/content/5ccf65ef-ae48-402c-9fd4-deeaf579c158

Razzano, G. (2016). *Connecting the Dots: The coordination challenge for the Open Government Partnership in South Africa*. Making All Voices Count, Open Democracy Advice Centre. https://www.makingallvoicescount.org/publication/connecting-dots-coordination-challenge-open-government-partnership/

Thieulin, B. (2019). *Towards a European Digital Sovereignty Policy*. Economic, Social and Environmental Council. https://www.lecese.fr/en/publications/towards-european-digital-sovereignty-policy