Data Governance in Zimbabwe: Opportunities and Challenges

Key Points

- **Recent legislation on data linking national security and cybersecurity undermines the creation of a trustworthy data environment.**
- **Restrictions on information flows have immediate and medium-term costs to digital economic activity, which in turn have knock-on effects for the prospect of any subsequent tax revenue.**
- **Extended economic instability is the main limiting factor for the growth of a digital society, but other limiting factors can be alleviated with mild targeted reform.**
- **A new policy agenda is required for the state to aid Zimbabweans to improve their life-chances, livelihoods and wellbeing with digital means.**
- **A policy framework to create enduring, affordable access through infrastructure extension and reliable connectivity can allow Zimbabweans to trade their goods and services online.**
- **These actions can help realise the principles of the African Declaration on Internet Rights and Freedoms and facilitate Zimbabweans innovating within the global digital economy.**

Introduction

Digitisation has had a broad impact on social and economic activity all over the world. Lawmakers know this. Through incremental and revolutionary surges in technology products, ubiquitous general computing capacities with network technologies like high-speed data transfer capabilities combine to allow actors to track human actions better. It has become routine for many states and corporations to quantify, record, measure, monitor and analyse this data.

To simplify this phenomenon, whether from commodifying audience attention or improving business intelligence, much value has been extracted to produce extraordinary

wealth, the bulk of which is concentrated with shareholders in the Global North (United Nations Conference on Trade and Development, 2019). The rollout of artificial intelligence and machine learning technologies will quicken these processes, bringing quantitative and qualitative changes that lawmakers need to anticipate if benefits are to be equally shared (Timcke, 2021).

Zimbabwe's digital transformation fits the general pattern of the African experience. Hardly anyone used the Internet in the year 2000; by 2020, 29% of the population did. Mobile cell phone subscriptions were two per 100 people in 2000; by 2020 they were 89 per 100 (see Figure 1). Now platforms like WhatsApp, Facebook and Twitter have become popular and ordinary.

These social changes have afforded an engaged citizenry to experiment with digital technologies on matters of public concern (Karekwaivanane & Mare, 2019; Karekwaivanane & Msonza, 2021) despite consumer data being historically expensive, especially when compared to neighbouring countries (see Figure 2). While the envelope for the exercise of political rights online does expand and contract, a thorough explanation of the history and development of Zimbabwe's political context is beyond the scope of this brief but can be found in Karekwaivanane (2017).

"By the year 2020, 29% of the population used the internet while mobile cell phone subscriptions were two per 100 people."

Taking into account the fast adoption rates of internet and various data-driven technologies, Zimbabwean lawmakers can be commended for making strides in data governance over the past five years. The country put key pieces of legislation in place during periods of intense factional contests, a prolonged democratic contraction and economic recession, and repeated mobilisation of security forces against dissenters.

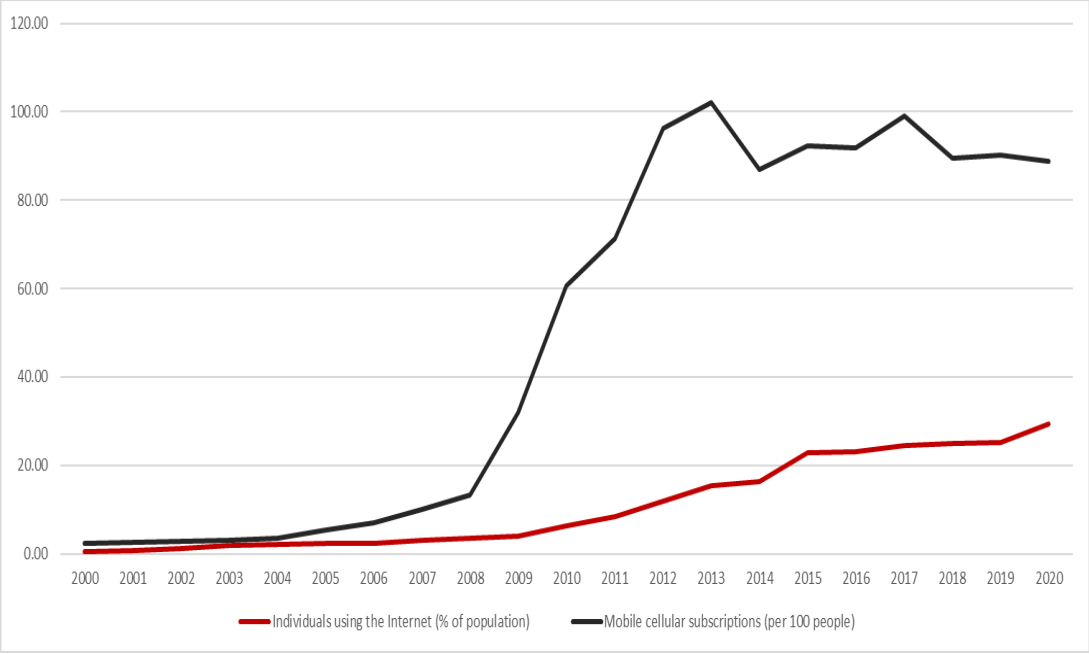

Figure 1: Adoption of Internet and mobile subscriptions, 2000 – 2020; data from the World Bank.

Presently the Government of Zimbabwe's 2021 to 2025 National Development Strategy 1 aims to rejuvenate economic conditions so that the country can become an "Empowered and Prosperous Upper Middle-Income Society by 2030". Recognising the importance of digitalisation, the authors of the National Development Strategy 1 dedicate a chapter to the issue. These and other broader considerations need to be taken into account if Zimbabweans are to create conditions for equitable social and economic development by participating in the digital economy.

The Legal Context

The Cyber Security and Data Protection Bill

In 2019, Zimbabwe's first attempt at formal data governance came in the form of the Cyber Security and Data Protection Bill. The Bill conflates cybersecurity and data protection. The Bill sought to establish oversight mechanisms over cybercrime and data by establishing a Computer and Cybercrime Committee to oversee the implementation of law and policy related to cybercrimes and security and a Data Protection Authority to oversee data handling issues in the country. The preamble encouraged technological development and the "lawful" use of technology, a loaded term given how successive Zimbabwean governments have used the law to suppress rights (Moyo, 2011). The preamble further provided for investigation and collection of evidence of cybercrime and unauthorised data collection and breaches; provided for the admissibility of electronic evidence for such offences; and encouraged a technology-driven business environment. Following consultations and debates the Bill did not pass parliamentary scrutiny. The main reason was to align with regional (Southern African Development Community [SADC]) standards that legally separate cybercrimes and data protection.

The Cyber and Data Protection Act

This experience led to the present Cyber and Data Protection Act of 2021 (CDPA). The Act focuses on data protection while addressing cybersecurity through amendments to existing cybercrime and evidence laws like Chapter VIII of the Criminal Law (Codification and Reform) Act that deals with computer-related crimes, the Criminal Procedure and Evidence Act as well as the Interception of Communications Act. The goal of the CDPA also changed from what was first thought of in the Cyber Security and Data Protection Bill, which was focused on making sure that technology was used legally.

Instead, the CDPA prioritises data protection "to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects". The Act's primary concern is data privacy and ensuring data protection for any data obtained by data handlers both inside and outside of the nation if the mechanism used for processing is located in Zimbabwe. Data controllers must process data fairly and lawfully by ensuring that data is collected only for specified, explicit and legitimate purposes, taking into account all relevant factors.

Some additional features of the Cyber and Data Protection Act of 2021:

- ❖ It mandates data handlers to actively seek consent in writing from the data subject to collect any sensitive personal data and outlines exceptions for when consent is not necessary.
- ❖ It requires data controllers to take appropriate technical and organisational measures to protect data from unauthorised destruction, negligent loss, unauthorised alteration or access and any other unauthorised processing of the data (security).
- ❖ It sets out cross-border data transfer requirements, i.e., personal data cannot be transferred outside Zimbabwe unless an adequate level of protection is ensured in the destination country.
- ❖ It establishes a Data Regulatory Authority which has all the necessary legal enforcement powers to ensure the CDPA is being enforced properly and a Cybersecurity and Monitoring of Interception of Communications Centre by repealing the Interception of Communications Act.

The Cyber and Data Protection Regulations

In 2022, the government introduced the Cyber and Data Protection (Licensing of Data Controllers and Appointment of DPOs) Regulations. Data controllers must obtain licences and designate a data protection officer according to these regulations. A Data Protection Officer (DPO) is tasked with a number of responsibilities outlined in the rules, including but not limited to:

- ❖ ensuring compliance by the data controller with the provisions of data protection law;
- ❖ dealing with requests made to the data controller by the Authority under the Act;
- ❖ informing and advise the employees about their obligations to comply with data protection laws;
- ❖ monitoring compliance with data protection laws, and with organisational data protection policies;
- ❖ advising on and monitor data protection impact assessments; and
- ❖ cooperating with the Authority and acting as the first point of contact for the Authority; and for individuals whose data is processed (employees, customers, etc).

Further legal refinement required.

It is encouraging that Zimbabwe is aiming to regulate data. However, the law needs further refinement. Despite calls to deal with cybersecurity and data protection separately, the Cyber and Data Protection Act remains an “omnibus” law dealing with multiple issues all at once. While these issues may be related, cybercrime, cybersecurity and data protection are unique areas that require particular attention to foster a safe digital environment in which data exchanges can take place.

Despite the Cyber and Data Protection Act seeking to create a data protection framework to guide data controllers, questions remain about the extent to which this framework will cater towards national security purposes. In a country where internet shutdowns are commonplace and free speech – both off and online – is stifled and prosecuted, the lack of public participation in data-related matters is concerning.

The Cyber and Data Protection Act creates protections for data processed in Zimbabwe, providing safeguards for sensitive data like health records. Still civil society groups drew attention to oversights and loose definitions that could be abused (Media Institute of Southern Africa Zimbabwe, 2020; Privacy International, 2020). There is scope to reinforce rights to privacy (Ncube, 2016; Privacy International, 2016). For a legal analysis of the constitutionality of state-deployed biometric identification technologies, see Ngwenya (2021).

Continuity and change

"While cyber security and cybercrime and data protection may be related, they are unique areas that require particular attention to foster a safe digital environment in which data exchanges can take place."

Abstracting from specific features of individual laws, there is an identifiable continuity between current legislative efforts and older frameworks like the Access to Information and Protection of Privacy Act (2002) as amended, and the Public Order and Security Act (2005) as amended. The former was meant to ward against data abuses by public authorities. Notwithstanding these social protections, the Government of Zimbabwe used these laws to curtail freedom of expression and digital civil rights (Moyo, 2011) much as the Interception of Communications Act (2007) compels service providers to give the state "real time and full time monitoring facilities for the interception of communications" (Section 9(c) Interception of Communications Act of 2007). Provisions like these were used to ban bulk SMS during the 2013 national election (Ndlovu, 2011). For a regional comparative analysis of the prior legislative package, see Khumalo, Mosweu & Bhebhe (2016).

In summary, the current laws may appear to be reformist, but subtly permit authoritarian exercises of power. For instance, the designation of the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) as the data protection authority consolidates power in one entity, thereby aiding political centralisation. The Cyber Security Centre, which will be located in the President's Office, will have the authority to issue warrants for communications interception, including interfering with private communications and data, as well as using search and seizure powers to access the information. Finally, the legal framework gives the post and telecommunications regulator, POTRAZ, criminal investigative powers in areas like cybercrime and monitoring public data processing. There is also a democratic deficit as stakeholders like independent information technology (IT) experts, IT enterprises, or members of civil society are not permitted to have representation in the Data Protection Authority.

Data governance can involve:

- Defining policies and procedures for data management, including guidelines for the collection, storage, access, and use of data.
- Establishing roles and responsibilities for data management, including stewardship, ownership, and conditions of use.
- Setting standards for data quality, including definitions of accuracy, completeness, and consistency.
- Implementing processes and tools for monitoring the quality of data.
- Establishing security controls to safeguard against unauthorised access or misuse.
- Providing training and resources to support suitable data management practices.

The data governance policy space

A combination of national policies, organisational procedures, and technical standards can be administratively leveraged to better specify roles, responsibilities and conduct of particular actors. These legal, commercial, and engineering components are complicated by the transnational character of data flows, meaning that digital trade necessarily involves working with several external partners and international bodies to ensure continuity and compliance.

Although shutdowns are imposed with high costs, the Zimbabwean Government has used them as a blunt data governance instrument. The NetBlocks Cost of Shutdown Tool estimates that the economic impact of an Internet disruption in Zimbabwe is nearly US$4 million per day, or ±Z$1.28 trillion. Put differently, that figure is roughly 0.015% of Zimbabwe's GDP in 2022.

Recently the Zimbabwean High Court ruled that an order for Internet shutdowns was unlawful as the incorrect functionary was used (*Zimbabwe Lawyers for Human Rights v. Minister of State, National Security*, 2019). However, the ruling did establish a binding and persuasive precedent about the use of power, even if not a forceful support of freedom of expression that the plaintiffs had wished for (Veritas, 2019). Nevertheless, cultivating a track record of political stability, especially during high visibility periods, can help improve the calculations for investment.

The roles of international, regional, and national institutions

In addition to national institutions, Zimbabwe's data governance environment is constituted by several different kinds of entities. Some of these are:

- international system for technical governance of the Internet, Internet Corporation for Names and Numbers (ICANN) and regional bodies such as the Asia Pacific Network Information Centre;
- international organisations like the International Telecommunication Union, the World Trade Organisation, and the UN's Commission on International Trade and Law;

- ❖ regional representative bodies like the African Union and SADC's Parliamentary Forum; and
- ❖ regional secretariats of the African Continental Free Trade Area (AfCFTA) and the Communications Regulators Association of Southern Africa.

While these entities share the goal of harmonisation for market integration, there are different ideas about what the end product should look like, and which model of data governance to pursue.

For Zimbabweans to improve their chances that the digital goods they produce can be traded on the Internet (or for them to add value in critical sectors) there is value in a whole-of-society push to respond to and join with global conversation about data governance.

" The economic impact of an Internet disruption in Zimbabwe is nearly US$4 million per day, or ±Z$1.28 trillion. Approximately 0.015% of Zimbabwe's GDP in 2022."

Can data sovereignty address neo-colonialism?

Some commentators argue that the declaration of data sovereignty can prevent neo-colonial relationships and unequal exchange from developing. Invoking citizens' rights to privacy and local commercial prospects through service substitution, data sovereignty advocates suggest that the state has the legal right to enforce entities to retain data within the national territory (see AU Data Policy Framework 2002, pp. 47-49). Secondary appeals to essentialist ontological categories are enrolled in arguments that vehemently oppose unequal exchange (e.g., Mawere & van Stam, 2020).

More practically, localisation of data storage allows identification of responsible parties, specification of security storage standards, as well as legal reach in cases of potential liability for data abuse (Hlomani, 2022). Enforcement techniques vary, although the construction of data centres is a common objective. In the case of Zimbabwe, Section 28 of the Cyber Security and Data Protection Bill of 2020 indicated an interest in limiting cross-border data transfers to third parties unless there are adequate protective measures in a foreign country. Zimbabwean officials could be more explicit about standards and enforcement of these protective measures.

The aggressive pursuit of data sovereignty can create friction with other established Internet operating principles, such as the free and open transmission of information (De La Chapelle & Porciuncula, 2021). In addition to hindering essential basic functioning of the Internet, there are risks that excessively stringent data sovereignty could lead to cloud-based services deciding to exit from markets as a national customer base may not be profitable enough to offset the cost of localisation. Zimbabwe's new government-operated National Data Centre is intended to address some of these issues, although it is too early to assess operational results.

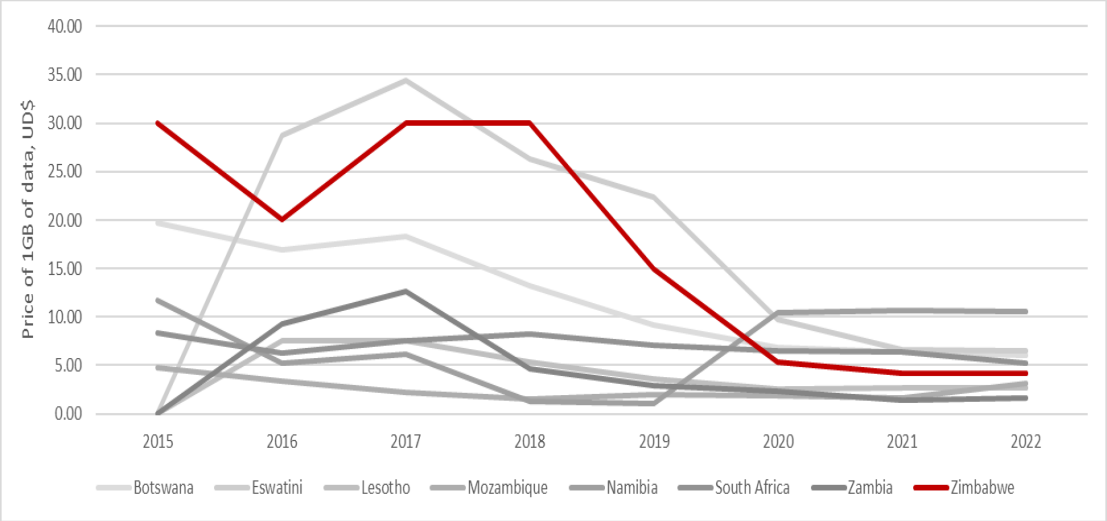

Figure 2: Price of 1GB data in US$ at the beginning of each year for selected Southern African countries. Data from Research ICT Africa (RIA) (2023).

How institutional decisions affect costs to users

"A conceptual shift is required in the policymaking arena to manage further integration with global networks better."

Zimbabwe was among the most-expensive countries in Africa for broadband data until recently (see Figure 2). These costs can partially be explained by high barriers to entry to the telecommunication market, the lack of competition in retail and wholesale markets, and a weak exchange rate for equipment procurement. Depending on specific class, an Internet Access Provider must pay US$5.5 million (±Z$1.8 billion) for an initial licence fee, a 2% (or US$100 000, whichever is greater) annual fee of audited annual gross turnover, and contribute 1.5% of audited annual gross turnover to a universal service fund (POTRAZ, 2022).

Some of these costs can be adjusted by mild institutional reform. Improving digital readiness is a task for all stakeholders, but policy goals that prioritise digital inclusion and connection will position Zimbabweans better to trade their goods and services online. Put simply, real accessibility is the prerequisite for inclusive innovation.

Due caution with open-data policies and digital state identification

An open-data policy is a set of guidelines, principles, and practices that outline how governments should make their data publicly available. Advocates suggest providing these goods for public benefit can lower costs for commercial products while simultaneously allowing for citizens to check and balance authorities (Kitchin, 2014). One downside of open-data policies is that a "mosaic effect" can be created by unreleased or missing information and in turn leading to false conclusions. Commercial exploitation can compound this "mosaic effect" as there is a financial interest in propagating a product or service that may only partially reflect reality.

Zimbabwean ministries reportedly are reluctant to share data with researchers, citing the possibility of abusive practices and infringement of intellectual property rights

(Chiparausha & Chigwada, 2019). Still, the Government of Zimbabwe has endorsed open-data frameworks proposed by non-governmental organisations (Chigwada, 2022). Caution should be exercised if steps are taken to create a coherent national policy. Aside from involving stakeholders to decide about the kinds of administrative data to make available for public and commercial use, advanced anonymising strategies must be a legislative component of any ethical open-data protocol.

There are efforts in Zimbabwe to establish a National Biometric Database to produce state identity documents like passports and certificates. These developments follow a 2018 project to create a biometric voter registration database for the Zimbabwe Electoral Commission. There have been leaks and/or data breaches of this database, with personal details being used by the ruling party for electioneering (Ngwenya, 2021). Similarly, given incidents where the national security forces used their military grade surveillance technology against citizens (Munoriyarwa, 2022), it is important that facial recognition systems and other biometric systems are not used to disable political participation and undermine social life.

Implications and recommendations

Building upon recent legislative developments, Zimbabwe's national strategy for data and society can be made more comprehensive to address costs of everyday connection. Efforts here include the need to safeguard better against data abuses without being unduly guided by assumptions that emanate from the state security cluster. Both issues need attention if the country wishes to receive the economic benefits of interconnectedness. Additionally, guaranteeing connectivity can boost confidence that there is sustained institutional commitment to trade and exchange.

A conceptual shift is required in the policymaking arena to manage further integration with global networks better. Policymakers need to appreciate that the era of managing discrete sectors has passed, and that changes in one area have cascading effects across the entire network (Razzano, et al., 2020). As digital societies and economies are not neatly confined within national boundaries, the enormous public and private benefits from digital transformation can only be realised when a country is willing to connect with existing networks so that people can interact and trade with others. Recognising this change of paradigm is especially important for policymakers who have spent decades debating the utility of decoupling from international markets that have cemented around unequal exchange.

References

African Internet Rights. (2020). African Declaration on Internet Rights and Freedoms. https://africaninternetrights.org/en/declaration

African Union. (2022). AU Data Policy Framework. African Union. https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf [in text as (AU Data Policy Framework 2022)]

Chigwada, J. (2022). Feasibility of a national open data policy in Zimbabwe. *Frontiers in Research Metrics and Analytics*, 12 August 2022, volume 7. https://www.frontiersin.org/articles/10.3389/frma.2022.985999/full

Chiparausha, B. & Chigwada, J. P. (2019). Accessibility of research data at academic institutions in Zimbabwe. In R. Bhardwaj, & P. Banks (Eds.), *Research data access and management in modern libraries* (pp. 81–89). Hershey IGI Global.

De La Chapelle, B., & Porciuncula, L. (2021). *We need to talk about data: Framing the debate around free flow of data and data sovereignty*. Internet & Jurisdiction Policy Network. https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf

Hlomani, H. (2022, October 29). More clouds over Africa: What will they bring? *RIA Blog*. https://researchictafrica.net/2022/10/29/more-clouds-over-africa-what-will-they-bring/

Interception of Communications Act of 2007. https://data.misa.org/api/files/1643273817060izd56r5tcwi.pdf

Government of Zimbabwe. (2020). *National Development Strategy.* https://www.dpcorp.co.zw/assets/national-development-strategy-1_2021---2025_goz.pdf

Karekwaivanane G., & Mare, A. (2019). "We are not just voters, we are citizens!": Social media, the #ThisFlag campaign, and insurgent citizenship in Zimbabwe. In T. Molony, & M. Dwyer (Eds.), *Social media and politics in Africa: Democracy, security and surveillance*. Zed Press.

Karekwaivanane, G. (2017). *The struggle over state power in Zimbabwe: Law and politics since 1950*. Cambridge University Press.

Karekwaivanane, G., & Msonza, N. (2021). Zimbabwe digital rights landscape report. In Tony Roberts (Ed.). (2021). *Digital rights in closing civic space: Lessons from ten African countries*. Institute of Development Studies. DOI: 10.19088/IDS.2021.003.

Khumalo, N. B., Mosweu, O., & Bhebhe, S. (2016). A comparative study of freedom of information legislation in Botswana, South Africa and Zimbabwe. *Mousaion*, 34(4). https://hdl.handle.net/10520/EJC-a2fd77a2f

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences.* SAGE Publications.

Media Institute of Southern Africa Zimbabwe. (2020, 19 May). Cybersecurity and Data Protection Bill entrenches surveillances.

https://zimbabwe.misa.org/2020/05/19/cybersecurity-and-data-protection-bill-entrenches-surveillance-an-analysis/

Moyo, L. (2011). Blogging down a dictatorship: Human rights, citizen journalists and the right to communicate in Zimbabwe. *Journalism* 12(6), 745–760. https://doi.org/10.1177/1464884911405469

Munoriyarwa, A. (2022). The militarization of digital surveillance in post-coup Zimbabwe: 'Just don't tell them what we do.' *Security Dialogue*, 53(5), 456–474. https://doi.org/10.1177/09670106221118796

Mawere, M., & van Stam, G. (2020). Data sovereignty: A perspective from Zimbabwe. In *12th ACM Conference on Web Science Companion*. Association for Computing Machinery. https://doi.org/10.1145/3394332.3402823

Ncube, C. (2016). Data protection in Zimbabwe. In A. Makulilo (Ed.). *African data privacy laws* (pp. 99-116). Springer.

Ndlovu, R. (2011, August 2). *Bulk messages banned in Zimbabwe*. Mail & Guardian. https://mg.co.za/article/2013-08-02-00-bulk-messages-banned/

Ngwenya, N. (2021). *Digital identity in Zimbabwe: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa* (Towards the Evaluation of Digital ID Ecosystems in Africa: Findings from Ten Countries) [Case study], Research ICT Africa. https://researchictafrica.net/publication/digital-identity-in-zimbabwe-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/

Postal and Telecommunications Regulatory Authority of Zimbabwe. (2022). Internet access providers. https://www.potraz.gov.zw/?page_id=424 [in text as (POTRAZ 2022)]

Privacy International. (2016). *The right to privacy in Zimbabwe.* Stakeholder report, Universal Periodic Review, 26th Session - Zimbabwe. http://hrp.law.harvard.edu/wp-content/uploads/2016/04/zimbabwe_upr2016.pdf

Privacy International. (2020). Submission on the Cyber Security and Data Protection Bill 2019 to the Parliament of Zimbabwe, June 2020. https://privacyinternational.org/sites/default/files/2020-07/Submission%20on%20the%20Cyber%20Security%20and%20Data%20Protection%20Bill%202019%20to%20the%20Parliament%20of%20Zimbabwe.pdf

Razzano et al. (2020). *The digital economy and society*. SADC PF discussion paper. Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2020/11/digital-economy-report_04.pdf

Research ICT Africa. (2023). Research ICT Africa mobile pricing (RAMP). Retrieved January, 10, 2023 from https://researchictafrica.net/research-ict-africa-ramp-index-2/

Romaniuk, S. N., & Burgers, T. (2018, October 18). *How China's AI technology exports are seeding surveillance*. The Diplomat. https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/

Timcke, S. (2021). *Algorithms and the end of politics: The shaping of technology in 21st century American life.* Bristol University Press.

United Nations Conference on Trade and Development. (2019). Digital economy report 2019 – Value creation and capture: Implications for developing countries. United Nations Conference on Trade and Development. https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

Veritas. (2019). Court watch 1/2019 – The Internet shutdown: The High Court's ruling of 21st January. https://www.veritaszim.net/node/3397

Zimbabwe Lawyers for Human Rights v. Minister of State, National Security (https://globalfreedomofexpression.columbia.edu/cases/zimbabwe-lawyers-for-human-rights-v-minister-of-state-national-security/ January 21, 2021).

_____

Authors

Scott Timcke: stimcke@researchictafrica.net

Hanani Hlomani: hhlomani@researchictafrica.net

Enquiries

Hanani Hlomani

Research ICT Africa

Workshop 17 | 17 Dock Road | V&A Waterfront | Cape Town, 8001 | South Africa |

T: +27 21 447 6332409