Digital Identity in Zimbabwe

Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa

RESEARCH & WRITING
Nhlanhla Ngwenya

REVIEW & EDITING
Anri van der Spuy, Vrinda Bhandari, Shruti Trikanad & Yesha Tshering Paul

COPYEDITING
Samantha Perry

COVER ILLUSTRATION
Akash Sheshadri

LAYOUT
Aparna Chivukula

RESEARCH ICT AFRICA

THE CENTRE FOR internet & SOCIETY

OMIDYAR NETWORK™

Digital Identity in Zimbabwe

Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa

A project of the Centre for Internet and Society (CIS), and Research ICT Africa (RIA)

→ digitalid.design ←
→ cis-india.org ←
→ researchictafrica.net ←

Digital Identity in Zimbabwe

By Nhlanhla Ngwenya, independent consultant

PREAMBLE

With an estimated 500 million people in Africa living without any form of legal identification (birth certificate or national ID),[1] the use of digital forms of identification has become increasingly popular because of their relative ease, low cost, and convenience compared to more analogue systems.

The Covid-19 pandemic has, if anything, increased the appetite for digital identification platforms and technologies.[2] The African Union Commission is currently working on a continental initiative to develop an interoperability framework for digital ID. Among other policy instruments, this effort draws its mandate from the *Digital Transformation Strategy* (DTS) *for Africa (2020-2030)*, which emphasises the importance of digitised legal identification mechanisms on the continent. The DTS highlights both the potential social and economic implications of digital IDs for Africans, noting that digital IDs not only support social development, but also enable meaningful participation in productive processes to generate economic growth, spur innovation, and support entrepreneurship. Besides being viewed as an enabler for realising all these policy objectives, digital IDs are seen as critical for the successful implementation of the African Continental Free Trade Area (AfCFTA).

With the growing enthusiasm for digital ID in Africa and across the world, there is a need to examine their impact on human rights, the rule of law, and the people who will be included (and excluded) from related systems. More critical analyses of digital ID's impacts in the global South, as well as the actors involved in designing and implementing them, are needed because digital identity programmes create an inherent power imbalance between the State and its people. The collection of personal data leave residents with little ability to exert

1 ID4D global dataset, 2018. See: *https://datacatalog.worldbank.org/dataset/identification-development-global-dataset*

2 Martin, Schoemaker, Weitzberg & Cheesman, 2021.

agency in its collection, storage and use, particularly when their right to privacy is not safeguarded or their personal data protected. And while increasing access to legal identification might appear to be a positive development for countries, this is not unequivocally the case.

In addition to the very real challenges of living without legal identification – whether digitised or analogue – those who *do* have digital do have digital identity may face other challenges. Experiences depend on (historical) context,[3] with some digital identities being developed in an attempt to segregate or even coerce people, while others are designed under the guise of national security concerns. Some countries have IDs that are no longer fit for purpose in a digital age,[4] while digitisation can also introduce novel harms. These include not only the direct risks associated with the collection and storage of personal data but arguably greater harms of exclusion or discrimination. Unless active measures are taken to counter such harms far from improving lives and potentially livelihoods, the introduction of digital ID systems could exacerbate inequality when analogue options are discarded – especially in African contexts with low connectivity levels.

On the other hand, digital identity systems, like all ICTs, are actively designed and shaped and therefore not inevitably detrimental from a developmental, human rights, and/or inclusion perspective.[5] If digital identities are conceived and designed with human rights, developmental goals, sustainability, and safety at the forefront, they might have a more transformative impact for the continent.[6] Critically examining the design, development, and implementation of these evolving systems remains crucial therefore, along with whether policymakers are doing enough (from a governance perspective) to ensure the positive outcomes of engagement with these socio-digital systems, while mitigating the risks that accompany many digital identities on the continent.

The Project

With this background in mind, Research ICT Africa (RIA) and the Centre for Internet and Society (CIS) partnered in 2020 and 2021 to investigate, map and report on aspects related to the state of digital identity in ten countries in Africa. The project looked at local (and digitised, in full or partially) foundational ID

3 Breckenridge, 2014.

4 African Union Commission, 2021.

5 e.g., Lievrouw, 2014; Parikka, 2012; Freedman, 2002; Wacjman, 2000; Williams, 1985.

6 c.f., Weitzberg, Cheesman, Martin, & Schoemaker, 2021.

systems in Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe.

The research took place within parameters set by an Evaluation Framework for Digital Identities[7] (the 'Framework'), which was developed by CIS with the purpose of assessing the alignment of digital identity systems for compliance with international rights and data protection norms. (CIS initially developed the Framework with a view of using it to assess India's Aadhar system, but the Framework has since been used in other contexts too.)[8] By using this Framework, the ten country partners evaluated certain aspects of the existing governance and implementation mechanisms of digital identity in their respective and unique contexts.

The Framework introduces a series of questions against which digital identity may be tested, aiming to address the various rights and freedoms that are potentially impacted by the state use of a biometric digital identity program. More detail about the Framework can be found in Annex II.

This report on the Zimbabwean case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Nhlanhla Ngwenya. Besides being an independent case study, the findings from this report were also used to inform a comparative report put together by the RIA and CIS teams to analyse the similarities, differences, and other aspects across the ten case studies – including key recommendations for policymakers, researchers, civil society actors, and other stakeholders.

An important limitation of the research is that the country case studies were conducted using the analytical lenses provided by the Framework, partly with the aim of assessing whether the Framework is relevant in African contexts, and might therefore not cover all aspects pertaining to digital identity in the context concerned. We elaborate on this limitation – which we feel significant in the contextually rich and diverse African context – in the comparative report.

PREAMBLE REFERENCES

African Union Commission (2021). *Draft AU Interoperability Framework for Digital ID* (August, 2021). [not published.]

Breckenridge, K. (2014). *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge: Cambridge University Press.

7 *https://digitalid.design/evaluation-framework-02.html*

8 *https://digitalid.design/evaluation-framework-case-studies/estonia.html*, *https://digitalid.design/evaluation-framework-case-studies/kenya.html*

Freedman, D. (2002) *A 'Technological Idiot'? Raymond Williams and Communications Technology, Information, Communication & Society*, vol. 5(3): 425-442.

Lievrouw, L.A. (2014) "*Materiality and media in communication and technology studies: An unfinished project*." In: Gillespie, T., Boczkowski, P.J., Foot, K.A. (Eds.) (2014) Media technologies: Essays on communication, materiality and society. London: MIT Press.

Martin, A.; Schoemaker, E.; Weitzberg, K. & Cheesman, M. (2021) *Researching digital identity in time of crisis (workshop report).* London: The Alan Turing Institute. Available at: https://www.turing.ac.uk/sites/default/files/2021-08/3c_workshop_reporttimes_of_crisis_.pdf

Parikka, J. (2012) *New Materialism as Media Theory: Medianatures and Dirty Matter, Communication and Critical/Cultural Studies, vol. 9*(1): 95-100.

Weitzberg, K.; Cheesman, M.; Martin, A. & Schoemaker, E. (2021) *Between surveillance and recognition: Rethinking digital identity in aid. Big Data & Society*, January-June: 1-7.

Williams, R. (1985) *Towards 2000*. Harmondsworth: Penguin.

ACKNOWLEDGEMENTS

This report was made possible by the support received from Omidyar Network. The Evaluation Framework referenced in this report was developed by the Centre for Internet and Society. The case study was conducted by Nhlanhla Ngwenya, with the support of Research ICT Africa (Anri van der Spuy and Naila Govan-Vassen) and the Centre for Internet and Society (Shruti Trikanad, Vrinda Bhandari and Yesha Tshering Paul). The RIA and CIS teams do not necessarily agree with the views expressed in this country case study. The authors thank the people who made their time and expertise available to contribute to and review this report.

ABSTRACT

Countries are moving to adopt digital ID systems to help address the exclusion of their citizens under the traditional analogue registration frameworks as well as ensure access to basic services, including healthcare, education, social welfare and voting.

As this has progressed, challenges around full registration of citizens have persisted while new risks and threats to citizens' rights have emerged. This is more prevalent in some African countries, including Zimbabwe, whose digital ID programme is still at an introductory stage and only partially implemented.

Aside from the foundational ID framework, which many Zimbabweans have experienced, there is little information available on digital ID systems in the country. The few times that the topic has been publicly mentioned, it has been in the context of the government announcing sectoral and functional systems, such as registration of civil servants or updating the voters' roll. Even then, there is insufficient public awareness of the systems, let alone transparency around data collection, purpose, usage, storage and destruction.

This paper derives from research and analysis of the state of digital IDs in Zimbabwe and examines how the programme complies with principles and standards relating to data protection and the promotion of human rights. As there is no overarching law governing digital IDs in Zimbabwe, this case study used the Centre for Internet and Society's Evaluation Framework to test the extent to which the country's proposed Cyber Security and Data Protection Law complies with human rights principles on digital IDs. If enacted, this law will guide the storage and processing of data including digital IDs.

The research shows that the country's legislative framework is weak and largely fails the three-tier checks, namely rule of law tests, rights-based tests and risk-based tests. The paper then makes recommendations on how the situation could be improved, starting with ensuring mass and inclusive registration of all Zimbabweans, and progressing to enactment of an overarching law anchored on human rights principles to guide the governance of digital IDs.

ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
BVR	Biometric Voter Registration
CIS	Centre for Internet and Society
DPA	Data Protection Authority `
EU	European Union
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICT	Information Communication Technology
IMF	International Monetary Fund
JFCT	Justice For Children Trust
MISA	Media Institute of Southern Africa
MNOs	Mobile Network Operators
NDS 1	National Development Strategy 1
OECD	Organisation for Economic Co-operation and Development
POTRAZ	Postal and Telecommunications Authority of Zimbabwe`
RBZ	Reserve Bank of Zimbabwe
RG	Registrar General
SADC	Southern African Development Community
ZANU PF	Zimbabwe African National Union Patriotic Front
ZEC	Zimbabwe Electoral Commission
ZimStats	Zimbabwe Statistics Agency`
ZHRC	Zimbabwe Human Rights Commission
ZPRS	Zimbabwe Population Registration System

CONTENTS

INTRODUCTION

Zimbabwe has a population of more than 14.86 million people.[9] It is located in southern Africa and is a member of the Southern African Development Community (SADC). The country is landlocked and shares its borders with South Africa, Botswana, Mozambique and Zambia. Slightly more than a third of the country's population is estimated to be living in cities, while the majority resides in rural areas.[10]

Having gained independence in 1980 from British colonial rule, Zimbabwe is a constitutional democracy with a clear separation of powers exercised by three arms of the state - the Executive, the Legislature, and the Judiciary. This is anchored on the 2013 Constitution,[11] which was voted by the majority of Zimbabweans to replace the 1979 post-colonial charter crafted at Lancaster House in the UK (popularly known as the Lancaster House Constitution) as part of the peace settlement between the liberation movement and the colonial regime.

Although the country now has a progressive constitution, since independence the security sector - particularly the military - has played a significant role in the governance of the country, to the extent of subverting constitutional authority in some cases.[12] According to academic and former government minister Jonathan Moyo, the military is "the centre of state power in Zimbabwe. It is the system".[13]

The country's politics has had a negative effect on the economy. For instance, due to years of political instability, the Zimbabwean government borrowed huge amounts from the International Monetary Fund (IMF) in 2014, resulting in the national debt accounting for 50%of the country's GDP that year (expected to rise to above 7% in 2022).[14] The outbreak of the Covid-19 pandemic has added a further strain to the three-digit inflationary economy already hit by a series of droughts and devastating cyclones.[15] Like elsewhere in the world, the pandemic

9 See *https://worldpopulationreview.com/countries/zimbabwe-population* [accessed 1/06/2021]

10 See *https://www.statista.com/topics/4353/zimbabwe/* [accessed 1/06/2021]

11 See *https://www.parlzim.gov.zw/component/k2/download/1290_da9279a81557040d47c3a2c27012f6e1* [accessed 1/06/2021]

12 Rupiya, M (2011), The Military Factor in Zimbabwe's Political and Electoral Affairs: *https://www.semanticschol:ar.org/paper/The-Military-Factor-in-Zimbabwe%E2%80%99s-Political-%26/7287e99e7347cb686a4b893e24888acb296c1f2a*

13 Moyo, J (2019), *Excelgate: How Zimbabwe's 2018 Presidential Election Was Stolen*, Sapes Books: Harare

14 See: *https://www.statista.com/topics/4353/zimbabwe/* [accessed 7/06/2021]

15 See: *https://www.worldbank.org/en/country/zimbabwe/overview* [accessed 7/6/2021]

has disrupted livelihoods and added 1.3 million to the number of people in extreme poverty in Zimbabwe, pushing the figure to 7.9 million in 2020, which represents 49% of the population.[16]

Although the government has repeatedly blamed the country's poor economic performance on targeted sanctions imposed on members of the ruling elite,[17] civil society and the opposition have attributed the economic meltdown to autocratic rule, corruption and abuse of human rights.[18]

The government has attempted to address the economic malaise under its 2021-25 National Development Strategy 1 (NDS1), which it hopes will lay the groundwork for its ambitious plans to transform Zimbabwe into a middle-income country by 2030.[19] According to the World Bank, for that to happen, the government will have to adopt domestic policies that support price stability, make optimal use of public resources, minimise wasteful spending, ensure greater transparency and accountability; and increase public financing, among other measures.[20]

It is under NDS1 that the government announced several technological developments, including the establishment of a repository of government data, the National Data Centre,[21] and plans to set up a National Biometric Database for the production of e-passports, national IDs and birth certificates.[22] According to the government, the National Biometric Database project is designed to help increase passport production capacity to clear the backlog locally and at embassies in foreign countries.

This development will have an impact on the country's national identity registration framework, which is still largely based on the traditional analogue system that was partially digitised recently. Details of the system are outlined in the next sections of this paper, which first introduces the Zimbabwean approach to identification procedures before using the evaluation framework for assessing it.

16 See: note 11 above.

17 See https://www.irishtimes.com/news/mugabe-blames-sanctions-for-zimbabwe-problems-1.832354 and *https://www.aljazeera.com/economy/2019/10/25/thousands-in-zimbabwe-denounce-evil-western-sanctions* [accessed 7/06/2021]

18 See: *https://www.theafricareport.com/19293/zimbabwe-corruption-and-patronage-do-more-damage-than-sanctions/* [accessed 7/06/21]

19 See *https://www.herald.co.zw/development-strategy-1-launch-set-for-today/*

20 See *https://www.worldbank.org/en/country/zimbabwe/overview* [accessed 7/6/2021]

21 See *https://www.datacenterdynamics.com/en/news/national-data-center-zimbabwe-opens/* [accessed 5/6/2021]

22 See *https://www.biometricupdate.com/202106/zimbabwe-contracts-for-biometric-passports-production* [accessed 5/6/2021]

METHODOLOGY

A number of research methods were used. Secondary data analysis was used to examine existing legislative instruments and other policy documents guiding the governance of national IDs as well as digital IDs. This was done to provide a clearer understanding of the legislative landscape, which in the process helped with the identification of gaps, strengths, weaknesses and opportunities in the country's legislative framework on digital IDs. Also as part of secondary data analysis, a literature review was conducted to provide an understanding of existing research, debates and findings in the field of digital IDs. In addition, the researcher conducted interviews with selected individuals about the country's digital programmes, as well as public servants who had experienced the biometric registration of their personal information as part of the government's efforts to audit the civil service. All the data and information gathered was then used to test the human rights compliance of the digital ID framework against the evaluation framework.

EVOLUTION OF NATIONAL ID

Zimbabwe's national ID system has its roots in its colonial legacy and has evolved through the post-independent politicisation of citizenship law[23] and the realities of migration. Although the country has reformed its laws since it gained independence in 1980, the conceptual framework of digital ID, as well as the administrative application thereof, remains steeped in this colonial legacy.[24]

Controversies surrounding citizenship - including who has the right to vote among those with dual citizenship, descendants of the white settler community, and black immigrants from neighbouring countries - have particularly dogged post-independence Zimbabwe.[25] This is at least partly because the "new" state inherited a system of population control and registration from the colonial regime, whose pillars were anchored in privileging the minority white settler community, while dehumanising and disenfranchising local inhabitants as well as black immigrants, who were often abused for cheap labour.[26]

Although the new constitution (adopted in 2013) affirmed three categories of citizenship (citizenship by birth, by descent and by registration) to address

23 Manby, B. (2019), Report on Citizenship Law: Zimbabwe, GlobalCIT: European University Institute

24 See *https://cadmus.eui.eu/bitstream/handle/1814/60436/RSCAS_GLOBALCIT_CR_2019_01.pdf?sequence=1* [accessed 5/6/2021]

25 See note 19 above.

26 See note 19 above.

exclusion and statelessness, challenges persist. These forms of citizenship had been confirmed through prior amendments to the citizenship law, with a 2009 modification being the main one.[27] Challenges include a lack of effective birth registration mechanisms; the centralisation of registration; the high cost of registration; as well as the poor provision of identity documents, among others.

For example, while birth registration and birth certificates are free for those born in Zimbabwe to the country's citizens, it costs USD 25[28] to register a child born in the country to non-citizens or for people who do not have documentation to prove they are citizens.[29] The correction of information and replacement of identification documents cost between USD 10 and USD 35. These fees are high in a country where 49% of the population is classified as poor[30] and thus create grounds for potential exclusion for a significant number of people from the national registry. People seeking Zimbabwean citizenship who are not of Zimbabwean descent are charged USD 5 000, irrespective of whether they are an adult or a child[31].

The registration system has also perpetuated the colonial classification of citizens that allows for population control and likely discrimination based on their ethnicity and place of origin. These issues have already been blamed for the partisan allocation of national resources and development.[32] They are also reflected in the identification numbers assigned to individuals, which show citizenship by birth or naturalisation, as well as district of origin, which is, in most cases, a rural constituency.

Just like in many other countries in Africa, the issuance of national identity documents is a statutory requirement in terms of the National Registration Act (Chapter 10:17), which came into effect in 1976 but has been amended a number of times (through Acts 36/1976; 41/1978; 17/1979; 1/1984; 14/1994; and 22/2001). The Act regulates the collection, use and storage of the national

27 *Ibid.*

28 The US$ which has been used as legal tender since 2009, though the Zimbabwe government has since ordered the use of the local currency for all transactions and services at the going exchange rate. See *https://www.voazimbabwe.com/a/zimbabwe-introduces-stiff-foreign-currency-penalties-of-up-to--five-million/5907587.html*

29 See note 21 and Zimbabwe Registrar General Website *http://www.rg.gov.zw/index.php/services/birth-and-death-certificates* [accessed 8/6/2021]

30 See note 12 above

31 See note 23 above

32 Ndhlovu, G.N (2019), The Ethnicity of Development? Discourses Shaping Developmental Politics in Rural Matabeleland South, Zimbabwe, In *African Journal of Social Work: AJSW*, Volume 9 Number 1 2019.

database. It provides for the registration of persons resident in Zimbabwe with identity documents, such as national identity cards and passports.

The Registrar-General of National Registration established under the Act is responsible for the processing of identity documents and for verifying the authenticity of supporting documents submitted in an application. A facial image and fingerprints are also required during the registration process and are included on the identity card, along with a unique identity number (assigned upon registration at birth and also included in a birth certificate issued in terms of the Births and Deaths Registration Act [Chapter 5:02]). Birth certificates are therefore a prerequisite and mandatory for the registration of an identity document. In 2001, the government introduced the "long" birth certificate, which includes details of the country of origin of the parents of the bearer of the birth certificate,[33] and against which other identity documents can be obtained. This is mandatory and a lack of documentation for parents can, by extension, mean their children may not be registered.

Besides the lack of documentation by parents, some other factors have also affected registration. Research conducted by the Justice For Children Trust (JFCT) in 2007 revealed that some of the factors for exclusion include ignorance of the registration framework, processes and procedures; long distances to registration centres; lack of bus fare to travel to the centres; bureaucratic requirements and unprofessionalism at the registration centres; and patriarchal traditional beliefs that hindered women from registering their children without the consent of a man.[34] The requirements that there be witnesses with national identity cards and a witness letter for children born in poor communities such as on farms, are other challenges that have been cited as reason for lack of birth registration and, in turn, the exclusion of people living in outlying areas from joining the national registry.[35]

Although the government has increased the number of birth registration centres around the country to address some of the above mentioned challenges,[36] using the birth certificate as the main prerequisite for national registration has caused serious problems. For example, hundreds of people in Zimbabwe's southwestern

33 Research and Advocacy Unit (2008), A Right or a Privilege: Access to Identity or Citizenship in Zimbabwe, Harare.

34 See: *http://archive.kubatana.net/docs/chiyou/jct_birth_registration_0710.pdf* [accessed 5/6/2021]

35 See: *https://www.streetchildren.org/legal-atlas/map/zimbabwe/legal-identity/can-a-child-obtain-retroactive-or-replacement-birth-registration-documents/* [accessed 5/6/2021]

36 See: *https://bulawayo24.com/index-id-news-sc-national-byo-113401.html* and https://www.thenewhumanitarian.org/news/2005/02/11/decentralised-birth-registration-nets-more-children [accessed 5/6/2021]

provinces of Matabeleland (consisting of three provinces: Matabeleland North, Bulawayo metropolitan, and Matabeleland South) do not have identification documents because their parents were killed in the post-independence massacres (dubbed Gukurahundi, meaning in Shona "the early rain which washes away the chaff before the spring rains") of opposition supporters. These people have been unable to have their birth certificates processed.[37] As explained by Amnesty International:[38]

> *Traumatised survivors had to grapple with the challenges of statelessness as they are required to produce death certificates as proof of their parents to apply for Zimbabwean nationality. However, death certificates for people killed in the Gukurahundi operation were not issued, meaning those who were orphaned as a result of violence had no way of proving their parents' nationality.*

An estimated 300 000 Zimbabweans, including descendants of the Gukurahundi victims, are currently at risk of being stateless and some feel like they are "stray animals"[39] because they are undocumented. As a result, their children are unable to access education, women are excluded from critical life-saving health care and assistance during labour as they cannot produce a national ID, and the majority cannot participate in the political process or engage in entrepreneurial activities.[40]

However, it is not only victims of state-sponsored ethnic cleansing and political violence that have been left in limbo. There are recorded cases of blatant discrimination against women getting identification particulars of their own or for their children. Although there are no specific requirements for men, women have in the past not been registered for "failing" to meet certain bureaucratic requirements such as: "... women should not have artificial hairstyles..." or that "...married women needed to change their surnames to that of their husbands..." if they need to gain access to official documents, including passports and birth certificates for their children.[41] (By artificial hairstyles, the registration authorities meant synthetic braids and hair extensions, among other hair pieces sometimes

37 See: *https://www.dailymaverick.co.za/article/2020-08-19-the-loveless-fatherless-stateless-generation-this-is-the-legacy-of-rapist-and-murderer-black-jesus-perrance-shiri/*

38 Amnesty International (2021), Zimbabwe Statelessness crisis traps hundreds of thousands in limbo, See: *https://www.amnesty.org/en/latest/news/2021/04/zimbabwe-statelessness-crisis-traps-hundreds-of-thousands-in-limbo/*

39 See note 35 above

40 *Ibid.*

41 See note 2 above.

preferred by women for cosmetic reasons.)

Individuals of foreign descent who have been resident in Zimbabwe their entire lives have also been affected by the politicisation of the citizenship law. Ahead of the 2002 elections, for example, the government amended the law to categorise these individuals as "aliens" who are not entitled to some of the political rights guaranteed to citizens.[42] This move was seen as an attempt by the ruling party to disenfranchise farm workers, especially those who had emigrated from neighbouring countries such as Mozambique, Malawi and Zambia and were perceived to be supporters of the main opposition party.[43] However, the "new" 2013 Constitution, which replaced the 1979 Lancaster House Constitution, has restored citizenship to those who had lived in Zimbabwe all of their lives but were considered alien because they were born of foreign descent.[44]

As a part of centralising and digitising the population registry, the department of the Registrar General integrated a computerised system called the Zimbabwe Population Registration System (ZPRS) in 1996. The system is a centralised composite database with a wide area network spanning the entire country.[45] According to the department, the purpose of the system "is to secure the data and help the department to support functions as per different Acts of Parliament administered by the department".[46] The database contains all demographic personal data collected related to registration of birth, death, national identification (ID number, full name, date of birth, village of origin, place of birth, date of issuance and signature), marriage, and passport. This data is shared for e-governance purposes, including with pension offices, the government salaries bureau, the immigration and police departments, the Zimbabwe Statistics bureau, the motor vehicle registration system, as well as with the private sector through businesses such as mobile phone service providers and banking services. District and provincial registrars can retrieve data and make changes to the database instantly. The government has announced that citizens can now apply for identification documents online.[47] However, there will still be a need for in-person processing of the application, to allow for the collection of information

42 See: *https://static.pmg.org.za/docs/2003/appendices/030603draftzimreport.htm* and *https://cadmus.eui.eu/bitstream/handle/1814/60436/RSCAS_GLOBALCIT_CR_2019_01.pdf?sequence=1* [accessed 5/6/2021].

43 See: *https://www.hrw.org/reports/2002/zimbabwe/ZimLand0302-03.htm* [accessed 7/6/2021].

44 Section 43 of Constitution of Zimbabwe Amendment (No 20).

45 Republic of Zimbabwe Production of Machine Readable Documents presentation by Department of Registrar General, November 2012.

46 See note 2 above.

47 See *https://www.biometricupdate.com/202106/zimbabwe-contracts-for-biometric-passports-production* [accessed 5/6/2021]

such as fingerprints.

As the government moved to embrace e-governance systems, it also embarked on the digitisation of the national ID after 1996. Since then personally identifiable information is stored in digital formats. When applying for an identity document, individuals are photographed, fingerprinted and have their details captured and stored in a database. Data captured for the purposes of the population registry include their full names, birth date and place, address, citizenship status (residents can also get certificate of registration of citizen upon meeting the requirements), date of entry into Zimbabwe, marital status, family particulars, and tribal affiliations as stipulated in the registration law.[48] While demands for family particulars and tribal affiliation were required under the colonial regime for implementing segregation policies based on race and ethnicity, it is not clear why the post-colonial state still retains this detail in the registration statutes. There is also no clarity on what is meant by tribal affiliations, which can be loosely interpreted as meaning the ethnic group one is born of and belongs to, or why this detail is necessary.

Biometric IDs were introduced in Zimbabwe in the early 2000s by the then Registrar General, Tobaiwa Mudede, as a formalised transition to reportedly enhance issues of e-governance.[49] Not only was there little publicity on this transition, limited information was made available about tendering and procurement processes, and no meaningful public consultation on the process took place. As a result, many people in the country are not fully aware of the implications of the new digitised ID features, and tend to believe that the primary difference is a new plastic ID card rather than the erstwhile metal ones (that were not biometric). Zimbabweans also do not seem aware of the implications of biometrics for the security of personal data. Research done by Engine Room in 2019 shows that it is only when citizens were made aware of the fact that their personal data collected for biometric voter registration are in the hands of government that they appeared concerned[50]. This is perhaps a reflection of lack of trust in the authorities' personal data management, especially that which relates to elections, a perennially disputed process.

In 2018, the government embarked on a massive biometric voter registration drive through which personal data, including phone numbers, was provided

48 Section 6 of the National Registration Act Chapter 10:17

49 Republic of Zimbabwe Production of Machine Readable Documents presentation by Department of Registrar General, November 2012

50 Chair, C. & Majama, K. (2019), Digital IDs in Zimbabwe: A Case Study, Engine Room [See: *https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf*]

to the Zimbabwe Electoral Commission (ZEC). The collection of contact details and details of one's constituency led to the infringement of privacy rights when the information was used by the ruling ZANU PF party to send many citizens direct campaign messages via text messages (SMSs). Citizens were worried about how and why the ZEC allowed a third party, the ZANU PF, to access and use their personal data without their prior consent. In general, citizens in Zimbabwe appear to now be concerned about the vital data they share with public institutions such as hospitals as well as both private and government-owned mobile network operators (MNOs).[51][52]

FUNCTIONAL DIGITAL ID SYSTEMS IN ZIMBABWE

Zimbabwe has embarked on several projects to plug into the population registry for functional purposes. These include an audit of civil servants; the registration of mobile phone users; the payment of social welfare grants, including those meant to mitigate the effects of the COVID-19 pandemic for the most vulnerable; vehicle registrations; and a number of other government services.

While the exercise to digitise national IDs has helped with adding security features to the card (e.g., ultraviolet fluorescence, dynamically shifting ink, holograms, watermarks, fingerprints and security barcodes), the country is yet to have a digital foundational ID system. However, the national ID registry has been used for functional purposes such as elections, auditing civil servants, a mobile network users' registry and a vehicle ownership registry (among other uses), making it the bedrock of all forms of individuals' identification in the country.

The Ministry of Health has also announced that it will issue an electronic card, linked to a person's passport and national ID, with security features and a quick-response (QR) barcode that can be scanned for verification as Covid-19 vaccination authentication documentation.[53] The national ID, or another government-issued authentication document, such as a passport, is a prerequisite for Zimbabwean citizens to get vaccinated under the government's vaccination programme, which potentially excludes those without identification documents.[54] Yet, some citizens from other countries, such as South Africa, have

51 See note 9 above

52 Zimbabwe has three MNOs. Only one, Econet Wireless, is privately owned. NetOneis wholly owned by the government, which also has a controlling stake in Telecel Zimbabwe.

53 See: *https://www.businesslive.co.za/bd/national/2021-03-29-zimbabwe-to-issue-electronic-covid-19-cards/* [accessed 12/4/21]

54 See: *https://allafrica.com/stories/202107090332.html* [accessed 27/7/2021]

reportedly travelled to Zimbabwe to get vaccinated at a fee of USD 70 per jab[55] due to frustration over the slow pace of public vaccination in their countries.

What has been more concerning is a lack of transparency, accountability and public consultation and awareness in the implementation of some digital ID programmes. In 2018, for example, the country entered into a partnership with a Chinese company, CloudWalk Technology, for a facial recognition programme. This formed part of the firm's exploratory project to develop software that recognises dark-skinned faces,[56] thereby training AI programmes to mitigate racial biases. China is arguably ahead in the race with the United States to become the global AI leader, and is seeking to overcome the problem of underrepresentation of African people in big data sets derived from American, European and Asian data subjects.

In the next section, two examples that highlight how the foundational identification has been used to build functional IDs in the country are briefly examined. The first is the Chinese driven project to use Zimbabwean biometric data to improve facial recognition of African features and the Civil Servants audit.

a) Chinese facial recognition project

Zimbabwe's bilateral relations with China, which can be traced to the country's struggle for independence, have strengthened in the recent past. This is both by design and default: by default, as Zimbabwe adopted its "Look-East Policy" following a fallout with its erstwhile Western economic and trade partners over land redistribution and its human rights record; by design, as China expands its influence in Africa. This relationship has enabled Zimbabwe to mitigate some of the economic challenges wrought by sanctions imposed on it by some Western nations.[57] The result is exemplified by various infrastructural development projects and technical support,[58] as well as a substantial donation of Covid-19 vaccines,[59]making Zimbabwe one of the first African countries to kick-start a public vaccination programme.

From China's perspective, the investment in Zimbabwe aligns with its expansion of its global influence, especially in Africa, which it views as having untapped

55 See: *https://www.timeslive.co.za/news/africa/2021-05-08-vaccine-tourism-south-africans-cross-border-to-zimbabwe-for-covid-19-jab/* [accessed 8/6/2021]

56 See: *https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/* [accessed 13/4/21]

57 See *https://journals.sagepub.com/doi/abs/10.1177/0974928417749642* [accessed 10/6/2021]

58 See *https://www.herald.co.zw/just-in-ed-highlights-priority-projects/* [accessed 10/6/2021]

59 See *http://www.xinhuanet.com/english/2021-02/16/c_139745036.htm* [accessed 10/6/2021]

economic potential.[60] As a result, China is now Africa's biggest trading partner, with trade volumes worth about USD 200 billion a year, a value that is likely to grow following China's announcement of the creation of a USD 1billion infrastructure development fund for the continent under its Belt and Road Africa Initiative.[61] China is now Zimbabwe's number three trading partner, after South Africa and Singapore, with a trade value of more than USD 358 million a year.[62]

It is against this background that, in April 2018, the Government of Zimbabwe and a Chinese company, CloudWalk Technology, signed a deal to develop a mass facial recognition programme. The programme essentially gives the company access to a black racial mix of data that is much needed for the development and expansion of Chinese surveillance technology in what is deemed to be the first (known) Chinese AI project in Africa.

Citing the Chinese state newspaper Science and Technology, Foreign Policy reported that the deal will not only cover CCTV cameras, but includes "smart financial systems, airport, railway station and security and a national facial database".[63] Celebrating the deal struck under China's Belt and Road Initiative in Africa, Zimbabwe's Former Ambassador to China (and former advisor to President Mnangwagwa)[64] claimed that Zimbabwean authorities had approached their "all-weather friend" to "spearhead an AI revolution in Zimbabwe".[65] He noted that the benefits were not only to ensure smoother passenger processing at the country's border posts and points of entry, but to help the government build a smart financial and banking system. He reportedly contended that:[66]

> *An ordinary Zimbabwean probably won't believe that you can buy your groceries or pay your electricity bill by scanning your face, but this is where technology is taking us and as the government, we are happy because we are moving with the rest of the world.*

Although local authorities have described the project as a benign exercise

60 See *https://www.forbes.com/sites/wadeshepard/2019/10/03/what-china-is-really-up-to-in-africa/?sh=8ec528559304* [accessed 10/6/2021]

61 See note 53 above

62 See *https://wits.worldbank.org/countrysnapshot/en/ZWE* [accessed 11/6/2021]

63 See: *https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/* [accessed 13/4/21]

64 See *https://www.africaintelligence.com/mining-sector/2018/11/20/long-standing-mines-ambassador-christopher-mutsvangwa-out-of-action,108333141-art* [accessed 7/6/2021]

65 See: *https://allafrica.com/stories/201910090185.html* [accessed 12/4/21]

66 See note 11 above

meant to facilitate ease of doing business and improve services for citizens, the underlying potentially sinister motives are hard to ignore. Other Chinese firms such as Huawei already stand accused of facilitating the deployment of AI technology which could be used for surveillance purposes in other parts of Africa.[67] And expanding such technology on the continent potentially places China ahead of Western countries, as it could become the owner of one of the most expansive facial recognition databases that is more racially diversified compared to what is currently available.[68]

Similar technology has been provided in countries such as Uganda, where in 2019 the country's police confirmed the installation of a USD 126 million facial recognition infrastructure from Huawei as part of the company's Safe City initiative.[69] The project was also rolled out in Botswana, with 500 surveillance cameras being installed in Gaborone and Francistown in 2010 by Huawei Technologies to "secure life and property as well as countering terrorist activities effectively and efficiently".[70]

Given former President Mnangagwa's adviser's remarks on the intended wide usage of the technology, there is a risk it could also be applied systemically for social control, along the lines of the Chinese Social Credit system built on similar AI technology. Critiques of the system contend that it is disguised digital control mechanism which seeks to regulate behaviour and mass surveillance where the government tries to control every part of people's lives,[71] a practice the EU has considered banning in its proposed AI regulatory framework.[72]

Some fear that Chinese technologies will be used to undertake illegal surveillance of government opponents,[73] as has already happened elsewhere on the continent. For example, in 2019, Huawei engineers reportedly assisted Ugandan authorities to hack the WhatsApp and Skype accounts of the popular

67 See *https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa/* [accessed 5/6/2021]

68 See *https://globalvoices.org/2020/01/30/how-zimbabwes-biometric-id-scheme-and-chinas-ai-aspirations-threw-a-wrench-into-the-2018-election/* [accessed 11/4/21]

69 See *https://www.dw.com/en/huawei-africa-and-the-global-reach-of-surveillance-technology/a-50398869* [accessed 9/6/2021]

70 See *http://www.xinhuanet.com/english/2020-02/20/c_138799621.htm* [accessed 9/6/2021]

71 See *https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial* [accessed 27/7/2021]

72 See: *https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF* & *https://www.cnbc.com/2021/04/15/eu-considers-ban-on-ai-for-mass-surveillance-social-credit-scores.html* [accessed 27/7/2021]

73 See *https://www.dw.com/en/huawei-africa-and-the-global-reach-of-surveillance-technology/a-50398869* [accessed 9/6/2021]

local musician and opposition politician Robert Kyagulanyi Ssentamu (known as Bobi Wine).[74] In the same year in Zambia, Huawei technicians allegedly helped the government gain access to the communications of a team of bloggers running a pro-opposition news site, enabling police to track and arrest them.[75]

In Zimbabwe, concerns over such technology go beyond snooping to worries about it being used to disable political participation. In 2018, for example, some citizens expressed reservations about exercising their voting franchise following the country's adoption of a biometric voters' roll (BVR) to deal with the problem of "ghost" voters. Instead of the BVR being seen as a progressive development in addressing problems plaguing the voter register, it became a tool for voter intimidation.[76] Some voters felt the BVR was just another way authorities were trying to gather personal information about them, as they could easily be tracked down using their biometric details and addresses collected for voter registration.[77] The situation was worsened by reports of ruling party supporters going door-to-door, demanding serial numbers of registered voters' registration slips, along with their ID numbers. Citizens feared that this would help ruling party supporters detect how they voted.[78] This incident resulted in distrust of the BVR and the intimidation of some people, preventing them from participating in the elections.[79]

b) Civil servants' registration

In 2019, the Zimbabwean government announced that it was launching a biometric registration exercise for civil servants as a part of its reforms to restore order in the civil service by flushing out ghost workers.[80] The biometric registration exercise was done with the assistance of the World Bank as part of modernising the management of civil service in line with Zimbabwean government's Transitional Stabilisation Programme for economic growth.[81]

According to the chairperson of the Public Service Commission, the exercise

74 See *https://www.dw.com/en/huawei-africa-and-the-global-reach-of-surveillance-technology/a-50398869* [accessed 9 June2021]

75 See note 59 above

76 See *https://advox.globalvoices.org/2020/01/30/how-zimbabwes-biometric-id-scheme-and-chinas-ai-aspirations-threw-a-wrench-into-the-2018-election/* [accessed 10 June2021]

77 See note 68 above

78 *Ibid*

79 *Ibid*

80 See: *https://www.herald.co.zw/biometrics-to-weed-out-ghost-workers/* [accessed: 18 April2021]

81 See note 56 above

was to be conducted in three phases: the biometric registration of civil servants; the interfacing of captured data with the national biometric registration data; and the validation of data and system of integrity checks.[82] At the end of December 2020, the government announced that the process had resulted in the flushing out of about 10 000 ghost workers that were not "biometric compliant", meaning their particulars could not be matched on the population registry, nor traced at their work stations.[83]

Although the registration of civil servants was presented as a means to weed out non-existent government workers who were inflating the public service wage bill, it emerged that authorities were intent on using the biometrics authentication to monitor government employees, especially in light of their perennial protests over poor salaries and working conditions. For example, in the midst of a paralysing medical doctors' strike, former Health Minister Obediah Moyo told the country's Health and Child Care Parliamentary Portfolio Committee that the only way to ensure medical doctors reported for duty and were paid for the time that they went to work, was to impose a biometric registration on them to help with their clocking-in.[84] He told the committee:[85]

> *The Ministry of Health has determined that government policy as announced by the Ministry of Finance and Economic Development calls for biometric recording. This must be instituted at all government hospitals immediately. This will give the government the opportunity to pay its workers in accordance to attendance and performance at work.*

According to a school headmaster interviewed for this research, while biometric authentication would certainly help address some of the civil servants' pay roll challenges, the exercise was imposed upon civil servants. There was no consultation and no clear explanation being given as to who will have access to data, or how the data will be stored or used beyond cleaning up the wage bill.[86] His fears of the data being used for the surveillance of civil servants and crushing dissent in the public service appear to have been vindicated by the Minister of Health's submissions to parliament, cited above.

82 See note 19 above

83 See: *https://www.newzimbabwe.com/govt-dumps-10-000-ghost-workers/* [accessed 18 April 2021]

84 See: *https://bulawayo24.com/index-id-news-sc-national-byo-178869.html* [accessed 18 April 2021]

85 See note 22

86 Interview with a Headmaster in a Matabeleland North school who requested they are not named for fear of victimisation. Interview conducted on 13 April 2021

ANALYSIS OF ZIMBABWE'S DIGITAL ID SYSTEM

To examine how Zimbabwe was rolling out its digital ID programme, in particular the extent to which it complied with international instruments in protecting citizens' rights, the research will use an evaluation framework developed by the Centre for Internet and Society (CIS). The framework, which can be used to evaluate the governance of digital IDs across many countries, provides a series of questions against which digital ID may be tested to determine the legitimacy of uses based on fundamental rights and governing structure of the digital ID system.[87] Broken down into three tiers, namely, rule of law tests, rights-based tests, and risk-based tests,[88] the framework helps assess the adequacy of digital ID frameworks in protecting human rights across jurisdictions. The framework is useful both where digital ID systems already exist or where they are still being formulated and in the early stages of implementation, such as in Zimbabwe.

87 See *https://cis-india.org/internet-governance/blog/governing-id-introducing-our-evaluation-framework*

88 See *https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf*

THE RULE OF LAW

2.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

The framework for national identity in Zimbabwe is grounded in Chapter 3 of the Constitution of Zimbabwe Amendment (No. 20) Act, 2013 on Citizenship. There is no overarching digital ID or data protection law in Zimbabwe, despite sectoral use of digital ID. The Constitution states that:

> *.... all Zimbabwean citizens are entitled to the following rights and benefits, in addition to any others granted to them by law;*
>
> *a. to the protection of the State wherever they may be;*
>
> *b. to passports and other travel documents; and*
>
> *c. to birth certificates and other identity documents issued by the State.*

This constitutional provision is realised through the National Registration Act of 2001 (Chapter 10:17), which is the primary law that regulates the collection, use and storage of the national database of citizens' national identification register. The law specifies that all citizens, aliens and refugees should register for a national identity document.[89]

The Department of the Registrar General, which falls under the auspices of the Ministry of Home Affairs and Cultural Heritage, is responsible for issuing national identification documentation. Aside from the national identity card, the department is also responsible for the registration of births and deaths, citizenship, marriages, and cattle brands. It was also responsible for voter registration before that role was delegated to the Zimbabwe Electoral Commission after the adoption of the 2013 Constitution, which established the Commission.

In terms of Section 8 of the Act, the Registrar-General (RG) and all persons employed in that office, are responsible for the custodianship of information, and are required to keep secret all information in the exercise of their duties.[90] Section 8 (3) of the same Act stipulates that information in the custody of the RG can only be released by order of a court of law. Section 9 then provides for immunity to

89 See the National Registration Act of 2001 Chapter 10:17

90 Section 8 (1) (2) of the National Registration Act of 2001 Chapter 10:17

"the State, the Minister or the Registrar General or any other employee of the State for anything done in good faith and without negligence".

Parameters of "good faith" are not defined in the Act, thereby providing room for potential abuse. This is because there are no limitations to action undertaken in good faith and officers responsible for the safe custody of data can release it and use the defence of "good faith" to circumvent legal liability. While the presumption of good faith is a legal principle, it remains a challenge to disprove good faith and show malice or intent to do wrong or harm. Similarly, while the test of rationality such as the "reasonable-person test" can be used to assess if one acted without negligence, reasonability is highly subjective and contested.

According to Statutory Instrument No. 140 of 2009, which in Zimbabwe is a subsidiary legislation created by bodies or individuals under powers delegated to them by parliament,[91] individuals above the age of 16 years qualify to acquire a national ID. The law specifies that all citizens, aliens and refugees should register for a national identity document.[92] However, to acquire a national ID in Zimbabwe, one must possess a birth certificate. Zimbabwean birth certificates affirm one's date of birth, sex, and the identities of one's parents. The requirement that one first possess a birth certificate to get a national ID is problematic due to various factors that hinder access to birth registration documentation, some of which have been cited earlier in this paper.

Apart from these regulatory instruments, Zimbabwe has no single law regulating the collection and processing of personal information, including biometric data, for the purposes of digital IDs. Instead, several laws and policies have a direct impact on the right to privacy and protection of personal information as they relate to the specific activities and government processes. A selection of the more important of these are briefly discussed below:

The National Registration Act of 2001 provides for the registration of persons resident in Zimbabwe and for the issuance of identity documents and imposes obligations regarding the carrying of identity documents. It is through this Act that citizens obtain national identity cards. However, the law is silent on the nature of data collected during the process, and it does not clearly state whether the data will be collected biometrically or otherwise. Although the RG's office has now digitised its ID system, the law does not provide for the protection of the collected digital data and guidelines on the processing of the data as well as governing trans-border flow of the biometric data. These gaps are only covered by the Cyber Security and Data Protection Bill gazetted in May 2020, which on

91 See *https://zimlii.org/content/delegated-or-subsidiary-legislation* [accessed 8/ June 2021]

92 See: *http://www.rg.gov.zw/index.php/services/national-registration* [accessed 23 March 2021]

21 July 2021 passed through parliament and was sent to the Senate[93] for further debate.

The Bill, which if endorsed by the Senate will await presidential assent, is the most relevant to this study. With regards to having the necessary safeguards in place for the introduction of a biometric or digital ID, the Cyber Security and Data Protection Bill of 2020 is particularly pertinent. The intention of the Bill is to provide a framework for access to information, the protection of privacy of information, and the processing of data wholly or partly by automated means. The Bill prohibits the processing of sensitive information, as well as genetic, biometric, and health data except in specified circumstances, which include situations where the processing is necessary to comply with national security laws and for the prevention of imminent danger or the mitigation of specific criminal offences.

Section 19 of the proposed law, for instance, seeks to safeguard the data of citizens and provides that in the event of security breach, the data controller shall notify the Data Protection Authority (DPA) without any undue delay.

The Bill also promotes privacy and data protection in provisions that relate to cybercrimes, unlawful interference and interception of data and computer systems.

Of relevance to this study are the safeguards on transfer of data outside of Zimbabwe, which is provided for in Section 28. Section 28(1) states that a data controller may not transfer personal information about a data subject to a third party who is in a foreign country. Section 28(2) then stipulates that data may only be transferred if there is an adequate level of protection ensured in the country of the recipient or within the recipient's international organisation. While such provisions are common, especially among countries pushing for data localisation to ensure security of citizens' data, to strengthen cybersecurity, law enforcement and national security,[94] there is a need to ensure that the restrictions do not run counter to the realities of the free cross-border flow of data essential to the effective functioning of the Internet.[95] The impact of restrictions on information flow and sharing as well as the attendant socio-economic benefits[96] brought about digital trade and the data economy should be kept in mind.

93 See: *https://www.veritaszim.net/node/5177* [accessed 28July 2021]

94 See *https://www.oecd-ilibrary.org/docserver/7fbaed62-enpdf?expires=1623227801&id=id&accname=guest&checksum=500D3FA7744534034693D66A17A807FB* [accessed 9 June 2021]

95 See note 76 above

96 See *https://www.jdsupra.com/legalnews/data-localization-and-the-limits-of-5695264/* [accessed 9 June 2021]

Section 29, in turn, provides certain exceptions for the transfer of data to a country outside Zimbabwe. These exceptions arguably do not assure an adequate level of protection. The exemptions include data subject consent; protecting the interest of the data subject; processing data for the performance of a contract between the data subject and the controller as well as on vital interests and public interest grounds. There is arguably a need for further guidance on these exemption clauses so that "public and vital interests" are narrowly defined and interpreted to ensure that they are not broadly interpreted and open to abuse, thereby weakening the trans-border data protection offered in the proposed bill.[97] With the Bill now due for Senate debate, there is no longer an opportunity for the public to provide input, leaving its fate in the hands of Senators and, later on, the President, who has to sign it into law.

There are other national laws that relate to processing personal information. However, none of the laws (in existence or proposed) and policies substantively address both the opportunities and threats to personal information in the digital age, especially as this relates to digital IDs.

For example, the Zimbabwe National Policy for ICT (2016 to 2020)[98] has some elements related to data storage and transfer, which when looked at closely also impact on individuals' information held by both public and private bodies. It sets out the framework for the incorporation of e-government services. In the policy, e-government includes all electronic information movement, interactions and transactions that facilitate service delivery among government ministries, institutions, departments and agencies (G2G); between government and the private sector (G2P); and between government and the citizenry (G2C). The policy also states that e-government relies entirely on ICTs to provide services such as convenient access to interactive information and services, timely delivery of public services, and efficient and effective methods of conducting business transactions.

More importantly, the policy also provides for the establishment of a National Data Centre to "allow Zimbabwe to centralise her information storage, management and protection, as well as take advantage of cloud computing opportunities".[99] This Centre has since been established with the assistance of

97 See *https://privacyinternational.org/sites/default/files/2020-07/Submission%20on%20the%20Cyber%20Security%20and%20Data%20Protection%20Bill%202019%20to%20the%20Parliament%20of%20Zimbabwe.pdf* [accessed 9 June 2021]

98 *http://www.veritaszim.net/sites/veritas_d/files/Zimbabwe%20National%20Policy%20for%20ICT%202016.pdf*.

99 See note 29 above

the Chinese government, the Inspur Group of China and Sino Zimbabwe.[100] The government launched the Centre by presenting it as essential to anchor "all e-government programmes and will allow co-ordinated planning and monitoring of results".[101]

The Census and Statistics Act of 2001 (Chapter 10:29), in turn, regulates the collection of data and processing of national statistics during a census by the Zimbabwe Statistical Agency (ZimStats) as approved by the Minister of Finance or the Director-General. The Director-General has the responsibility of ensuring that results of any census or statistical survey are of good quality, are accurate and remain confidential.

Under the Act, ZimStats is mandated to collect, compile, analyse, interpret, publish and disseminate statistical information alone or in cooperation with other government ministries or institutions. In handling this information, ZimStats is required to develop and maintain a central business register and comprehensive national statistics database. Citizens are compelled to provide this information when asked to do so by authorised officers at the time.

A board is also established under the Act to monitor compliance of the agency with best practices and international recommendations on the production of official statistics. While the disclosure of information obtained from the field by officers of the agency is restricted, it authorises the minister to grant disclosure of information on terms and conditions they may specify. These are not specified in the law and may be misused.

Similarly, the Banking Act of 2015 (amended in 2016), Chapter 24:01, provides for the supervision and regulation of individuals and entities conducting business and financial activities in Zimbabwe. It defines banking activities as receiving deposits, travellers' cheques, credit cards and extending credit including mortgage credit and financing of financial transactions. It also contains elements of monitoring and supervision of banking activities, through the country's central bank, the Reserve Bank of Zimbabwe (RBZ). The Act obliges the preservation of secrecy in the protection of information acquired while performing their functions, except where disclosure is subject to approval by the RBZ. The disclosure of information concerning transactions, deposits and funds is permissible upon production of a warrant if it is required for detecting, investigating, or preventing an offence. However, the Act does not deal with the full protection of data collected by banking institutions in the exercise of their

100 *https://www.herald.co.zw/new-dawn-for-zim-as-president-launches-data-centre-to-anchor-govt-operations/* [accessed 28 April 21]

101 See note 31 above

duties. Instead, it permits the sharing of information between the RBZ, the Registrar and the Director of Census and Statistics whenever possible, for serving their respective functions.

Several incidents arguably demonstrate the potential misuse and abuse of personal information by government departments and businesses in Zimbabwe. A case in point is that of the publication of Zimbabwe's voter's roll in its entirety during the 2018 elections on an election portal hosted outside the country.[102] The incident demonstrated a breach in the privacy and protection of citizens' data by a third party, which used the data for a purpose it was not intended or collected for. This incident demonstrates flaws within existing legislation, which only addresses challenges with information held by public bodies but lacks provisions to deal with data breaches outside Zimbabwe's jurisdiction.

Evidently, though Zimbabwe has no national digital ID policy, sectoral government units have their own functional system(s) guided by specific administrative policies and laws. Some of these are grounded on the national population registry and all have an impact on citizens' rights to privacy and protection of personal information. For example, if authorities' claim that the CloudWalk facial recognition technology was a benign exercise meant to improve citizens' transactions and security[103] were true, the technology installed at borders and points of entry will be under the jurisdiction of the Immigration Department and its administrative laws. An interview with one intelligence operative indicated that although this is supposed to be the case, state security agencies are plugged into the data and have unhindered access for their own use.[104]

QUALITY OF THE LAW

Although Zimbabwe has no single overriding law governing digital IDs, the assessment of the National Registration Act of 2001 as the overarching legislative framework on national identification is relevant. This Act has the stated purpose to "provide for the registration of persons resident in Zimbabwe and for the issue of identity documents; to impose obligations regarding the carrying of identity documents; and to provide for matters connected with or incidental to the

102 Media Institute of Southern Africa Zimbabwe Chapter (2018). Zimbabwe's urgent need for data privacy laws. Retrieved 1 October 2019 *http://zimbabwe.misa.org/2018/07/13/zimbabwes-urgent-need-data-privacy-laws/*

103 See: *https://www.herald.co.zw/chinese-tech-revolution-comes-to-zim/*

104 Interview with central intelligence operative in Harare on 31 March 2021.

foregoing".[105]

The law then outlines the duties and obligations of the Registrar General (Sections 3,5 and 8); procedure and requirements for obtaining a national ID (Sections 6 and 7); liabilities of the Registrar General (Section 9); and offences for the violation of provisions of the law (Section 10). Section 11 provides wide and discretionary power to the responsible minister, in this case the Minister of Home Affairs, to "make regulations providing for any matter" required under the Act which in the minister's "opinion is necessary or convenient" to be provided for in giving effect to the law. Although the issuance of digital IDs could be inferred from Section 11 (2), which lists circumstances under which ministerial regulations could be provided for, all of the listed situations seemingly relate to the traditional identification documents. These include the issue of identity documents, whether original, duplicate or replacement, and the fees payable; the procedure for issuing identity documents; the surrender of identity documents issued to deceased persons; the correction of errors; alterations of particular appearance; and replacement of identity documents, among others.

Given the impact of digital technologies on individual identification, which has seen the increasing use of digital IDs, the Act is inevitably outdated. There is a need to review the law so that it incorporates these developments, if it is to be relevant as the overarching legal framework for the provision of national identification. As it is, the law is silent on the registration, issuance and usage of digital identification, which is being used in both public and private sectors. For instance, while the law establishes the office of the RG as the custodian of individual identification data, the use of digital identification systems in various sectors means that there are now several offices that have access to personal data harvested through the usage of those systems. This thus calls for a holistic review of the Act and other pieces of legislation to ensure harmonisation of the national identity registration and management framework. Such an exercise will likely also ensure there is alignment of roles and duties, as well as sufficient safeguards as it relates to collection of data, storage and usage of personal data (which is also done under the Electoral Act under which the biometric voters' roll is compiled).

As noted above, while Zimbabwe has no specific policy or law governing the use of digital IDs, the proposed data protection law has elements related to personal data central to digital identification. If enacted, the law will be critical in the management, usage and storage of digital data, and thus also warrants assessment regarding its alignment with international best practice.

Further, some issues and provisions in the Cyber Security and Data Protection

105 National Registration Act of 2001 Chapter 10:17

Bill are problematic. For instance, terms such as "data controller" are inadequately defined, while the term "critical data" is not defined at all (though it is widely used in the Bill). This may create problems in the interpretation of the Bill once it has been enacted, as these terms are open for wide interpretation. For example, "data controller" is narrowly (but inadequately) defined as: "any natural person or legal person who is licensable by the Authority". The definition should not be restricted to "licensable by the Authority", but should include any "natural or legal person, public or private, that, by itself or in association with others, decides the purposes and means of the processing of personal data"[106]

In addition, Section 7 of the Bill proposes the establishment of the Data Protection Authority. However, this would be an additional function assigned to the Postal and Telecommunications and Regulatory Authority of Zimbabwe (POTRAZ). The problem is that POTRAZ is not a fully independent body and this provision will lead to concentration of power in a single body already controlled by the government. To make matters worse, Section 8 of the Bill fails to give the Data Protection Authority (DPA) the powers to impose penalties, fines and enforcement mechanisms. This gap may mean the data controller could abuse an individual's data with minimal or no accountability due to weak deterrence measures.[107]

According to local civil society observers such as MISA Zimbabwe and Digital Society Zimbabwe, the proposed law falls short of sufficiently securing citizens' right to protection of personal data in its current format.[108] The organisations have made submissions to parliament and relevant ministries on parts of the Bill that need strengthening, such as Sections 3, 5, 6, 7 and 8, among others.[109]

Another issue raised by civil society pertains to the data subject's consent to having their non-sensitive, sensitive and genetic data, biometric sensitive and health data processed (outlined in Sections 12, 13 and 14 respectively). For example, Section 12 (3) provides for the processing of non-sensitive personal data without the consent of the data subject, when necessary under stipulated conditions. The exemptions are overly broad and allow for the processing of non-sensitive personal data for a variety of reasons.[110]

106 Privacy International.org. (2020). Submission on the Cyber Security and Data Protection Bill to Parliament of Zimbabwe

107 *Ibid*

108 Interviews with MISA Zimbabwe and Digital Society Directors in Harare on 5 March 2021.

109 See *https://zimbabwe.misa.org/2020/06/25/misa-writes-to-parliament-submissions-on-the-cybersecurity-bill/* [accessed 9 June2021]

110 See note 79 above

Specifically, under Subsection (12)(3)(d), it is unclear what is meant by processing data in the "public interest". As Privacy International contends, "public interest" is not defined in the Bill, leaving the provision open to abuse.[111] Similarly, Subsection (12)(3)(e) is unclear on what is meant by processing data on grounds of "legitimate interest" of the controller or a third party, also leaving the provision open to abuse.[112]

Section 14 of the Bill, which focuses on genetic, biometric sensitive data and health data, provides for the need for a data subject's consent before processing any data, but then lists 10 broad justifications for disregarding a data subject's consent, privacy rights, dignity and administrative justice. These reasons include processing the data to carry out the specific obligations and rights of the controller; to comply with national security laws; the promotion of public health; substantial public interest; and research, among others. As argued by Privacy International, the broad range of exemptions can lead to excessive exceptions for the need for consent for the processing of genetic, biometric and health data, which should be subject to higher safeguards.[113]

In its present form, the Bill may be misused by government departments and third parties, especially through processing the personal sensitive and non-sensitive data of citizens without their consent, a lack of effective oversight, or consideration of the rights of data principals. This would set a dangerous precedent that has no place in a data protection law.[114]

Although the government appeared to have paused the progression of the Bill since its gazetting in 2020, parliament resumed the debate in July 2021 and voted in favour of the proposed law, which was then sent to the Senate on July 21 for consideration. Should the Senate pass it, the Bill will be submitted to the presidency for assent.

CLARITY AND PRECISION

Several sections in the proposed Bill lack clarity and may therefore be subject to abuse by anyone with access to data, including digital IDs. For instance, Section 19 provides that data controllers have a mandate to notify the DPA of any data breach. However, it does not specify the exact time limits within which such a notice should be given. It only states that the breach should be reported without undue delay. This vagueness can potentially result in broad interpretation of the

111 *Ibid*

112 See note 79 above.

113 See note 79 above.

114 See note 104 above.

section, posing some challenges in implementing the law.

The attempt to define the scope of the Bill in Section 4 remains vague. Section 4(2)(a) refers to "effective and actual activities of any data controller" but does not define what these are, while Section 4(2)(b) states that the law will apply to "a controller who is not permanently established in Zimbabwe" but does not define what that means.[115] In addition, while the Bill mentions the issue of "critical data", it fails to define it.

Section 14 of the Bill governs the processing of genetic data, biometric sensitive data, and health data, which is strictly prohibited if done without consent from the subjects concerned. Consent is broadly defined in the Bill to refer to:

> "*any manifestation of specific unequivocal, freely given, informed expression of will by which the data subject or his or her legal, judicial or legally appointed representative accepts that his or her data be processed".*

However, the same section that governs consent also lists 10 exemptions for disregarding the data subject's consent, privacy rights, data dignity, and administrative justice in the processing of data.[116] Section 14(3) outlines these broad exemptions, which includes an exception relating to the processing of data necessary to carry out the specific obligations and rights of the controller in the field of employment law. Also included are exemptions on account of complying with national security laws; for the purposes of scientific research; and for the promotion of public health. Other exceptions relate to instances that are of "substantial" public interest as well as for the purposes of conducting medical examination of the population and preventing imminent danger, among other broad reasons that leave room for abuse.

2.2 LEGITIMATE AIM

Does the law have a legitimate aim? Does the law clearly define the purposes for which the ID can be used?

Currently there is no overarching law governing digital IDs in Zimbabwe against which the test of legitimate aim can be done. As stated above, the only law guiding the issuance and use of IDs in the country is the National Registration Act of 2001, whose aim and objectives regarding the registration of citizens is clearly spelt out in the law. However, some elements of digital ID governance, especially as it relates to

115 See note 103 above

116 Cyber Security and Data Protection Bill, 2019.

data storage, usage and processing, is covered under the proposed data protection law.

2.3 DEFINING ACTORS AND PURPOSE

Does the law governing digital ID clearly define all the actors that can use/manage or are connected to the ID database in any way?

To achieve the objective of protecting personal data, the proposed data protection Bill designates POTRAZ as the DPA. However, concerns have been raised about the independence of POTRAZ and whether it is the appropriate body for such a responsibility, given its other roles.[117]

The functions of a DPA should arguably be overseen by a statutory commission and an independent institution, whose appointment process is public and transparent enough to instil confidence and legitimacy. An independent DPA should also be accountable to Parliament. POTRAZ is created under the Postal and Telecommunications Act (Chapter 12:05) and currently has 15 functions in its portfolio, mainly relating to postal and telecommunications infrastructure licensing and economic regulation, though this is constantly expanding. While the DPA, as proposed in the Bill, can process complaints from data subjects as well as conduct inquiries or investigations on its own accord, it does not have the power to impose sanctions such as fines, enforcement notices, undertakings, and prosecution. This is problematic because it leaves the guiding framework with no stringent accountability mechanism to ensure stricter adherence to the law.

The Bill also establishes the data processor, who is referred to as a natural or legal person who processes data for and on behalf of the controller and under the controller's instruction. Data processors are found within both private entities and government agencies, as long as they process data on behalf of the data controller. The controller is also responsible for the "code of conduct", which the Bill defines as "data use charters", drafted to institute proper use of IT resources, the Internet, and electronic communications.

Actors: Who can use the digital IDs?

Although there is no policy regulating the use of digital IDs and specifications as to who can use them, there seems to be sectoral usage of the system in

117 *Ibid*

government services and in the private sector. These include banking, medical insurance as well as employee authentication by corporate entities. Immigration departments and security agents also reportedly have access to individuals' biometrics collected at the ports of entry and borders.

The Cybersecurity and Data Protection Bill does not distinguish limits imposed on private versus public usage of data. However, in terms of section 13 (c) of the bill, the Authority shall determine the circumstances in which the prohibition to process the data referred to in this section cannot be lifted, even with the data subject's consent, "taking into account the factors surrounding the prohibition and the reasons for collecting the data".

Thus, the Authority has the discretion to use its position to restrict or allow for the usage of data by both the public and private sectors if it deems necessary. This should not be left to the discretion of any authority and parameters for this should be laid down in the law.

2.4 REDRESS MECHANISMS

Does the law provide for adequate redress mechanisms against actors who use the digital ID and govern its use?

Both existing and proposed laws provide little to no redress mechanisms. Similarly, the proposed law does not specifically provide for redress mechanisms against actors who use and govern the use of digital IDs. However, in terms of Section 34(1) of the proposed legislation, any person aggrieved by the decision of the DPA may appeal to the Administrative Court. In addition, although the DPA can handle complaints by data subjects, Section 8 fails to give the DPA the power to impose sanctions on the offenders. This is a weakness which might compromise the security of data subjects.

In terms of Section 30(1), the DPA shall provide guidelines and approve codes of conduct and ethics governing the rules of conduct to be observed by data controllers and categories of data controllers. Since this is not provided for in the Bill but is to be later crafted by the DPA (which has been previously highlighted as lacking independence), the amount of trust and protection the code of conduct will inspire is questionable.

USER NOTIFICATION

To preserve the rights of data subjects, there should be provisions which compel legally designated custodians to notify data subjects of any breach or misuse of their data. Although the Bill points out that data controllers have a mandate to notify the DPA of any data breach (Section 19), it does not specify the exact time limits within which such a notice should be made. It only states that the breach

should be reported without "undue delay". Ideally, and in terms of international good practice, data controllers are mandated to notify users within 72 hours of any breach of their data.[118] As such, the Bill should also be clear about what will happen in the event of a breach and should prescribe the maximum time limit wherein a notification should be issued.

The processing of sensitive information (including genetic data, biometric sensitive data and health data) is prohibited under Sections 13 and 14 of the Bill. This implies that consent should be sought in the processing of personal and sensitive data. However, the need to notify data subjects through seeking consent is compromised by Sections 13 (2) and 14(2), which give the DPA permission to process data without seeking consent. For instance, exemptions covered under Section 13 (2) include the processing of data if it is necessary to carry out the obligations and specific rights of the controller in the field of employment law, if the processing of data is authorised by a law or any regulation for any other reason constituting substantial "public interest", and if the processing is necessary for the purposes of scientific research.

These sections must arguably be reviewed to protect data subjects against breaches of their privacy. Overly broad language and terminology - which may be used to unjustifiably process personal information without express consent - should be minimised, restricted and should not cause any prejudice.[119]

ACCESS AND CORRECTION

Section 15 (e)(iii) and 16 (e)(iii) of the Bill makes provision for data subjects to access and rectify data relating to them to ensure fair processing. These provisions can still be strengthened to ensure that, in addition to the rights provided for, citizens can also block or restrict the processing of data about them if it is inaccurate and incomplete. This would mean citizens can ensure no decisions are made about them on the basis of inaccurate information.[120]

The National Registration Act of 2001 also provides for correction of identification particulars. As there is no clarity on the linkages between digital IDs and the foundational law, however, it remains unclear whether citizens would be able to use the national identification framework to correct digital ID when the Bill is signed into law and becomes operational.

118 See *https://privacyinternational.org/sites/default/files/2020-07/Submission%20on%20the%20Cyber%20Security%20and%20Data%20Protection%20Bill%202019%20to%20the%20Parliament%20of%20Zimbabwe.pdf*

119 See note 103 above.

120 See note 94.

DUE PROCESS

In terms of Section 34(1) of the Bill, any person aggrieved by a decision of the DPA may appeal to the Administrative Court. However, although the DPA can handle complaints by data subjects, Section 8 fails to give it the power to impose sanctions on offenders or provide an effective remedy to data subjects.

This provision arguably does not meet international standards, as the independent supervisory authority should ideally have the power to receive complaints from data subjects and to investigate and impose penalties on the offenders. An independent supervisory authority should have the power to either sanction the violator within their own scope of powers or else refer the case to a court of law.[121] In addition, there should arguably be adequate and accessible mechanisms to compensate data subjects whose rights would have been violated by the authority, data processor or officer.

2.5 ACCOUNTABILITY

Are there adequate systems for accountability of governing bodies, users of digital ID and other actors?

Accountability issues are highlighted in Section 24 of the Bill, wherein the data controller is obliged to take all the necessary measures to comply with the principles and obligations set out in the proposed law. The data controller should also have the necessary internal mechanisms in place to demonstrate such compliance to both data subjects and the DPA.

However, this element of accountability is compromised under Section 20 of the Bill. For instance, Section 20(3) fails to detail what sort of registry should be exempt from the obligation to notify the DPA that they are processing personal data of data subjects.[122] On the other hand, exemptions from seeking consent from data subjects, such as processing data for "public interest" or "legitimate interest" (as outlined above) are not clearly defined, are vague, overly broad, and thus open to abuse.[123] This is because breaches in data protection may happen and be justified on the grounds that they occurred in the pursuit of promoting "public" or "legitimate" interests, which will remain abstract and contested if not precisely defined.

Further, the proposed law provides for accountability in the handling of

121 See note 103 above

122 *Ibid*

123 *Ibid*

data. This responsibility is given to the data controller, who according to Bill is "any natural person or legal person who is licensable by the Authority". Broadly applied, this could mean that both public and private actors can be data controllers as long as they are given authority by the designated DPA as established by law. Section 24 of the Bill enjoins the controller to take all necessary measures to comply with the principles and obligations set out in the law and to have the necessary mechanisms in place for demonstrating such compliance to both the data subjects and the DPA in the exercise of its powers. While the effort to build in accountability in the proposed law is commendable, it is the aforementioned lack of independence of oversight bodies (tasked with ensuring that the controller is accountable) that raises a lot of questions about the effectiveness of the accountability mechanism contained in the Bill.

The designation of POTRAZ as the DPA under Sections 7 and 8 of the Bill also potentially weakens the accountability mechanisms under the proposed law. The provision gives extensive powers to POTRAZ, a body that at law is more accountable to the executive than to the legislature and as such is not subject to robust parliamentary oversight. The Minister of ICT is empowered in law to make policy directions that must be complied with by the POTRAZ board.[124] Such powers affect POTRAZ's operational independence, given that it is not subject to parliamentary oversight and is only accountable to the executive.

Globally, the practice is to have separate and independent data authorities. For instance, in South Africa, the Information Regulator is an independent body established in terms of Section 39 of the Protection of Personal Information Act, No. 4 of 2013. It is subject only to the law and the country's Constitution. It reports to Parliament. The appointment process is transparent, interviews are carried out, Parliament recommends the appointment of members to the Regulator, and the public is invited to nominate members[125].

Although the South African case is beset with challenges (including a lack of adequate resources to fully execute its role), the principle of ensuring its independence is still instructive in modelling an independent body for Zimbabwe.[126]

Moreover, in terms of Section 32 of the Bill, the minister is given very wide-ranging powers, including making regulations that "in his or her opinion, are necessary or convenient to be prescribed for carrying out or giving effect to this

124 Sections 25 (3) and 26 (1)-(2) of Postal and Telecommunications Act

125 MISA Zimbabwe analysis of the proposed Cyber Security and Data Protection law (2020)

126 See *https://www.timeslive.co.za/news/south-africa/2020-10-08-information-regulator-wants-more-money-or-it-cant-do-its-job/* [assessed 9/6/2021]

Act". The powers given to the minister through this section should not be so broad as to bypass the powers of the DPA and thus evade scrutiny. This may severely compromise the Bill's accountability mechanisms, to the detriment of data subjects.

2.6 MISSION CREEP

Does the governing law explicitly specify the proposed purposes of the digital ID?

As noted above, Zimbabwe has no overriding law pertaining to the use of digital IDs despite evidence of the use of digital authentication by some sectors, both public and private. In addition to examples cited above , fingerprinting is used by a number of private entities to authenticate staff; digital identification systems are used by some medical insurance companies to authenticate their members; and digital identification systems are also used for vehicle registration, as well as for the compilation of the voters' roll.

All of these examples are implemented or administered under different policies guided by administrative and legislative frameworks relating to their respective sectors. For example:

- the voter registration and registry is guided by the Electoral Act, administered by the Justice Ministry, with ZEC responsible for the custodianship of the voters' roll, which was in 2018 transformed into a biometric register;
- the digital vehicle registry falls under the Ministry of Transport and Infrastructure Development, with the Central Vehicle Registry unit responsible for compilation, storage and use of data on individual and corporate vehicle ownership;
- some of the digital development projects that the government has announced in the recent past, such as the facial recognition programme by Chinese firms and the establishment of the national data centre, are led by the Ministry of ICTs under the government's national ICT Policy and Vision 2030. All of these have happened without an overarching legislative framework that would ensure transparency in individual data processing, storage and destruction as well as provide oversight and redress mechanisms for recourse.

There is little doubt that the proposed Bill is a step in the right direction regarding providing legislative safeguards to individuals' private data. The longer it is delayed, the longer citizens' data are vulnerable to political and commercial exploitation. In particular, Section 25 of the proposed law would help

to mitigate effects of projects such as the Chinese facial recognition programme, as it provides for the right of the data subject "not to be subject to a decision based solely on automated processing, including profiling, which produce legal effects concerning him/her or similarly significantly affects him or her". However, weaknesses in the Bill arguably undermine its stated intention and the government's obligations under the Constitution, as well as international law on the protection of human rights. The vagueness of clauses, wide discretionary ministerial powers and lack of independence of oversight bodies, among other legislative deficiencies, provide significant room for mission creep.

RIGHTS-BASED TESTS

The national ID law falls short in terms of fulfilling data protection principles requirements. For example, the law does not sufficiently provide for fair, lawful and transparent processing of personal data and neither does it categorically specify the need for compatibility of data processing with the purpose of collection. It does not set out clear minimisation of processing of data to limit it to the purpose for which it is being processed. Nor does it provide for storage limitations or strong accountability mechanisms for data processing. The proposed data protection law has sections that speak to these requirements and below is an assessment of the extent to which it accords with the principles.

3.1 NECESSITY AND PROPORTIONALITY

Are the privacy violations arising from the use of digital ID necessary and proportionate to achieve the legitimate aim?

The national ID law does not sufficiently build in principles of digital ID law that would ensure strict compliance with the principle of necessity and proportionality to guarantee that only personal data which is adequate and relevant for the purposes of the processing is collected and processed. In actuality, wide discretionary powers are given to the national Registrar General and the responsible minister on data storage and its processing, which is open to potential abuse. However, should the Bill pass into law, it will plug the gap; the Bill's Part IV (on Quality of data and the General Rules on the Processing of data under Sections 9 to 11, and 24) upholds internationally recognised principles of data protection.[127] Still, there is a need to address some elements of the proposed law to ensure proportional and legitimate processing of data. Sections below discuss some of the gaps that will need to be addressed for the proposed law to fully align with data protection principles and adequately safeguard citizens' rights.

127 See note 103 above.

3.2 DATA MINIMISATION

Are there clear limitations on what data may be collected, how it may be processed and how long it is retained for, during the use of digital ID?

There is no digital ID law that prescribes what information should be collected for the purposes of processing a digital ID. However, an assessment of the Bill shows a desire to limit the amount of data collected, as well as how long it is retained. Section 9 (1) provides that the data controller shall ensure that data collected should be:

> (a) adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;
>
> (b) accurate and, where necessary, kept up-to-date;
>
> (c) retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed.

The effectiveness of such provisions is, however, dependent on the quality and strength of the law as a whole. This is because the provisions cannot be read in isolation, but must be read with other sections of the law. Given the aforementioned weaknesses of the Bill, such minimisation may be a symbolic gesture rather than actually regulating the amount of data collected, its usage and retention. This is particularly so given that the proposed law is silent on how long data should be retained, and when and how it should be destroyed once the purpose has been fulfilled.

The proposed legislation also fails to provide clear limitations on who can access and process data. Section 17 vaguely stipulates that "[a]ny person having access to the data and acting under the authority of the controller or of the processor, as well as the processor himself or herself, may process data only as instructed by the controller, without prejudice to any duty imposed by law".[128]

Other weaknesses in controlling access are further outlined in the next section.

128 Section 17 of the proposed Cyber Security and Data Protection Bill

3.3 ACCESS CONTROL

The proposed Bill and existing legislation fail to provide guaranteed protections in the event that data is harvested during the creation and use of digital IDs. There are indications of public concerns[129] around the notion that agreeing to enrol for a biometric ID automatically translates to consent for the government to share personal data with various public and private entities for surveillance.[130]

However, adequate, informed, valid and unconditional consent should be sought before the processing of data, as guided by global data protection principles such as the African Union Convention on Cyber Security and Personal Data Protection,[131] the OECD Guidelines on the Protection of Privacy, the GDPR Principles on Data Protection,[132] and the United Nations Development Group's Data Privacy, Ethics and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda.[133] A lack of adequate protection of personal data held by government bodies such as the Registrar's Office raises concerns about the safety and security of data, as there is a risk citizens' data is being shared and processed without their consent.[134] These concerns are likely to persist if the proposed Bill is to pass as currently worded. Sections 13 and 14 of the Bill, in particular, erode the need to seek consent first from data subjects before data is processed or shared in some instances.

3.4 EXCLUSIONS

Are there adequate mechanisms to address exclusion from the system?

The national digital ID system in Zimbabwe has excluded some groups of society from the national registry and, by extension, from accessing basic services and fully participating in the country's political and socio-economic programmes. This is largely because of difficulties in accessing registration offices in Zimbabwe due to the centralisation of registration; the long distances people have to travel

129 See note 7 above

130 *Ibid*

131 See the AU Convention on Cyber Security and Personal Data protection *https://www.opennetafrica.org/?wpfb_dl=4*

132 See *https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf* [accessed 9 June2021]

133 See *https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf* [accessed 9 June2021]

134 See *https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf* [accessed 9 June 2021]

for registration; a lack of knowledge on the requirements to get registered; and cultural and patriarchal hindrances.[135] Other challenges include the failure to collect birth records from local health facilities to enable the process of getting birth certificates. Some research indicates that local clinics do not release birth records if, for example, the maternity care fees are not paid and, in fact, hold the record until a new mother or her family clear the debt.[136] This has seen a significant number of poor people left unregistered and thus stateless. They are unable to access basic services, social welfare grants, or participate in the country's political and socio-economic processes, which is then passed on to their children and generations after them.

In other cases, especially those instances where children are born in rural communities and outside the formal health centres, parents are required to bring witnesses for the registration of births. This is an added financial burden for poor communities, as they have to sponsor witnesses to get to the registration centres by paying for their bus fares, accommodation and food.[137]

As noted, patriarchal values, traditional beliefs and myths are also barriers to registration of children at birth. For example, some women are reportedly reluctant to register their children in their maiden names in cases where the father was not available or has denied paternity, for fear of possible cultural and traditional repercussions in future, such as the wrath of an "avenging spirit" from the man's ancestors.[138] Besides social and traditional factors, the cumbersome processes, inefficiency and unprofessionalism at the registration offices, which result in applicants enduring long queues and ill-treatment, have also contributed to lack of registration.[139] Registration centres are also at times hampered by resource constraints, such as a lack of equipment, consumables, office infrastructure and staff accommodation, which compromises the quality of services provided.[140]

The Zimbabwe Human Rights Commission's (ZHRC) inquiry into access to documentation revealed that there is often neglect and marginalisation of people living with disabilities and members of minority groups, such as the San, Tonga and Doma communities living in remote areas and on the margins of the

135 See *http://archive.kubatana.net/docs/chiyou/jct_birth_registration_0710.pdf* [accessed 5 June 2021]

136 See note 2 above

137 See note 113

138 *Ibid*

139 *Ibid*

140 Zimbabwe Human Rights Commission Report on National Inquiry on Access to Documentation in Zimbabwe; *http://www.veritaszim.net/sites/veritas_d/files/Report%20on%20National%20Inquiry%20on%20Access%20to%20Documentation%20in%20Zimbabwe.pdf* [accessed 10 June 2021]

government's developmental programmes.[141] It is difficult for these groups to access registration centres, let alone obtain identity documentation.

Since all digital identification is predicated on the foundational national ID, it means there is potential exclusion of the above groups in the national population registry due to the stated difficulties in accessing documents for registration, resulting in a single point of failure.

The ZHRC inquiry made extensive recommendations to mitigate challenges pertaining to birth registration. Among those is a call to the government to

- review legislation and policies so they are sensitive and responsive to the local context and community realities;
- increase resource allocation to the registration department for improved services;
- increase the number of registration centres in marginalised communities to enhance accessibility;
- heighten civic education on birth registration to empower communities with information on procedure and documentation for registration; and
- rope in traditional and local leaders to keep records of children born in their areas for authentication when they need registration documentation and witnesses at a later stage.[142]

Traditional leaders can also be used to debunk the traditional myths about entrenched patriarchy, which hinder the registration of children in some communities. There is also a need for enhanced inter-ministerial cooperation and coordination among institutions - such as the ministry of home affairs, ministry of health and child care, department of the Registrar General and the department of social welfare[143] - with the mandate to facilitate processing of documentation. .

Government has tried to respond to some of the challenges by periodically launching mobile registration centres to cater for those left out or facing challenges in obtaining documentation.[144] It has also announced its plans to leverage digital technology to boost the registration and production of

141 See note 123

142 *Ibid*

143 See note 118 above

144 See *https://bulawayo24.com/index-id-news-sc-national-byo-113401.html* [accessed 5 June 2021]

documentation for citizens in Zimbabwe and the diaspora.[145] Technology will certainly help those living in urban areas and living outside the country (if they have access to connected ICTs). However, the interventions are least likely to adequately address the registration challenges faced by rural and marginalised communities, the majority of whom are either unconnected or, if there is broadband availability cannot afford to go online. (Internet penetration in Zimbabwe stands at 33.4%[146] and the country has one of the most expensive data costs in Southern Africa at USD 2 a 1GB for daily usage.)[147]

3.5 MANDATORY USE

Are there valid grounds for mandatory participation, if such participation exists?

There are no mandatory requirements for the use of digital IDs to access services in either the private or public sector. The National Registration Act of 2001, which provides for the issuance of a national ID, imposes obligations regarding the carrying of identity documents for authentication,[148]but there is no specification as to the nature or type (biometric or non-biometric) of registration. Therefore, everyone issued with a new ID from the Registrar in the past five years is presumed to have a digitised ID. Both digital and non-digitised IDs appear to be in use without any problem in Zimbabwe. Other forms of identification, such as passports and drivers' licences, are also widely used.

145 See *https://allafrica.com/stories/202105270318.html* and https://allafrica.com/stories/201907050364.html [accessed 10 June 2021]

146 See *https://datareportal.com/reports/digital-2021-zimbabwe* [accessed 11 June 2021]

147 See *https://prepaid-data-sim-card.fandom.com/wiki/Zimbabwe* [accessed 11 June 2021]

148 National Registration Act [Chapter 10:17] Retrieved from *https://www.law.co.zw/download/1744/#:~:text=AN%20ACT%20to%20provide%20for,or%20incidental%20to%20the%20foregoing*

RISK-BASED TESTS

4.1 RISK ASSESSMENT

Are decisions regarding the legitimacy of uses, benefits of using digital ID, and their impact on individual rights, informed by risk assessment?

The use of biometric identity cards offers many advantages but also presents some challenges around privacy and the ability of citizens to control their digital information. There are two major risks which may affect the use of digital ID in the country. First, the misuse or use of biometric data for other purposes than those agreed to by the citizens, perpetrated either by the service providers or the fraudsters.[149] This risk is heightened by the fact that once biometric data is in the hands of a third party, it can be used for other purposes than that which the person consented to. While some citizens are aware of this risk, they still share their personal data, primarily because they are in need of services, either from government or private entities.

A second risk is that of re-use of data presented for biometrics. This happens when captured biometric data - during transmission to the central database - can be fraudulently replicated in another transaction.[150] Unfortunately, the proposed Cybersecurity and Data Protection Bill does not contain sufficient provisions to mitigate these risks and there is no evidence that a risk assessment was done prior to drafting the Bill, which is currently before the Senate.

Although Section 28 of the Bill states that the data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the country of the recipient or within the recipient's international organisation, the risk is heightened by Section 29. This section is worrisome because it permits the transfer of data to a country outside Zimbabwe which does not assure an adequate level of protection, under the guise of "public and vital interests".[151] The security of data is compromised under such circumstances and risks are heightened, given that the terms "public interests" and "vital interests" are not

149 Thales. (2021, April 6). Biometrics: definition, use cases and latest news. *https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics*.

150 *Ibid.*

151 See note 104

defined. To reduce the risks surrounding the use of data and digital IDs, data should never be transferred to any country outside Zimbabwe without adequate levels of protection.

Currently, there are no other provisions in any statutes which govern the use of digital IDs. Thus, there is a risk of misuse of the digital data obtained during the process of issuing these IDs. As has already been alluded to in the earlier discussions, the National Registration Act of 2001 does not cover issues around digital IDs. This leaves the data subjects vulnerable and their digital data legally unprotected.

4.2 DIFFERENTIATED APPROACHES TO RISK

Do the laws and regulations envisage a differentiated approach to governing uses of digital ID, based on the risks it entails?

With Zimbabwe still to transition into a fully functional digital ID system, risks related to use of digital identification are minimised by the fact that alternative identification documents - such as analogue traditional ID, passports and drivers licences - are often permitted for individual authentication.

4.3 PROPORTIONALITY

Does the law on digital ID envisage governance, which is proportional to the likelihood and severity of the possible risks of its use?

As cited above, Section 14 (3) of the Cybersecurity and Data Protection Bill contains exemptions to consent on processing of genetic, biometric sensitive and health data. For instance, Section 14 (3) (a) exempts consent in writing if processing is in compliance with national security laws, or (d) processing is required by or by virtue of law or any equivalent legislative act for reasons of substantial public interest, or (e) processing is necessary to protect vital interests of the data subject, or another person, or if the (g) data relates to data made public by the data subject.

To constitute a legitimate and justifiable exemption, this provision should be expanded to ensure that exemptions are clearly defined and prescribed by law. It should state that this legitimacy must be grounded in the advancement or respect for individual rights and freedoms under the country's Constitution. Similarly, "public interest" should be outlined clearly and also with sufficient safeguards for data protection and privacy.

4.4 RESPONSE TO RISKS

Does the governance regime provide strategies for dealing with risks, once they arise?

In the case of high risk from the use and abuse of digital IDs, the Bill does not specify clear mechanisms for prohibition or restriction. Section 16 deals with disclosures when not collecting data directly from the data subject. Subsection (1) states that "to safeguard the security, integrity and confidentiality of the data, the controller or his or her representative, or the processor, shall take the appropriate technical and organisational measures that are necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or access and any other unauthorised processing of the data".[152]

To ensure this, the Bill outlines security measures to be adopted, taking into account four specific issues, namely the state of technological development, the cost of implementing the measures, the nature of data to be protected, and the potential risk to data subjects. According to Section 18 (3) to 18(5) of the proposed law, the data authority may issue "appropriate standards" relating to information security for all or certain categories of processing. These sections also mandate the data controller to provide sufficient guarantees regarding the technical and organisational security measures to protect the data and to enter into a written contract or any legal instrument with the data processor to maintain security measures on data. The specifics of the measures are left at the discretion of the DPA, data controller and data processor and not specified in a law that provides sufficient safeguards against illegitimate processing.

Considering this, specifically the link between the security measures to be adopted and the potential risk to data subjects, the authorities may not necessarily prohibit the use of digital IDs. However, a fitting option would be to adopt new technological measures to counter the risks, if the cost of doing so would be less than the cost of data vulnerability and breaches in the use of digital IDs.

Such measures will help to ensure adequate responses to breaches, unlike in the past, as demonstrated by the manner in which the government responded to the leakage and use of personal data ahead of the 2018 elections. In that case, the ruling party, ZANU PF, was accused of sending unsolicited text messages to individuals and numbers registered on the mobile networks database as part of

152 Cyber Security and Data Protection Bill, 2019.

its election campaign.[153] The Post and Telecommunications Regulatory Authority of Zimbabwe issued a statement denying it had shared the data with political parties and insisting it had, in effect, banned the practice.[154] The Zimbabwe Electoral Commission, responsible for keeping the voters' roll secure, also denied it was involved and placed the blame on mobile networks.[155] As the two state institutions appeared to abdicate responsibility, one citizen had to approach the courts for relief,[156] arguing that the ZANU PF bulk SMS incident violated his consumer rights.[157] (The court was yet to pass judgment on the matter at the time our research was conducted.)

153 See *https://www.techzim.co.zw/2018/07/zanu-pf-sends-new-bulk-smss-thanking-recipients-in-advance-for-voting-for-ed-mnangagwa/* [accessed 9/6/2021]

154 See *https://businesstimes.co.zw/zanu-pf-admits-sending-out-bulk-sms/* [accessed 9/6/2021]

155 See note 112 above [accessed 9/6/2021]

156 See *http://www.tellzim.com/2018/07/masvingo-lawyer-drags-zec-econet-to.html* [accessed 9/6/2021]

157 See *https://ifex.org/election-related-breach-of-personal-information-reinforces-critical-need-for-data-privacy-laws-in-zimbabwe/* [accessed 9/6/2021]

CONCLUSION

Evidence on the ground shows that while Zimbabwe is yet to fully digitally transform its identification system, some forms of functional digital identification systems already exist in the country. These have been set up without a guiding legal framework that is in line with international normative frameworks or human rights laws, but within various pieces of legislation governing the administrative operations and functions of different sectors. Consequently, none of the laws and policies substantively address both the opportunities and risks to personal information in the digital age, especially as this relates to digital IDs. This has left citizens susceptible to abuse of their rights, with no effective recourse.

Although the government has tabled a Cyber Security and Data Protection Bill before parliament, which, if enacted, will provide some guidance on the storage and usage of data, including digital identification, the proposed law will not sufficiently safeguard citizens' rights to privacy.

Given this policy window and the opportunity to provide public input to the draft Bill, this is also a valuable opportunity for Zimbabwe to learn from other jurisdictions that have adopted digital IDs. What is required, is the political will and public service leadership that will subordinate paranoia of citizens' dissent to a genuine desire to build a just and an inclusive society where all citizens enjoy fundamental freedoms and entitlements due to them.

The paper thus recommends the following:

1. Legislation: As some sectors in Zimbabwe are using some forms of digital IDs, it is important that the country enacts an overarching legal framework to guide the issuance of the same IDs to enhance transparency, accountability and the protection of citizens' rights. In formulating such a law, Zimbabwe should conduct a comprehensive audit (including that of risks) of the legislative framework, to bring all policies and statutes relating to digital IDs together and ensure a harmonised legislative framework that can prevent abuse.
2. Public consultation: In reviewing legislation, there must be genuine public consultation to ensure citizens and all relevant stakeholders make meaningful contributions in the formulation of the law, which is essential in building trust between duty bearers and right holders in the application of the law.

3. Government: There is a need for the government to revisit the proposed Cyber Security and Data Protection Bill and incorporate submissions made to Parliament by civil society groups and other international bodies to protect the security of citizens' data.
4. Civil Society: There is a need for civil society groups to heighten their push for alternative and democratic legislation that governs national IDs and digital IDs to ensure there is inclusion of all groups of society in the country's population registry. This would go a long way in ensuring just and fair access to basic services.
5. Inclusion of women and marginalised communities: There is need to implement the Human Rights Commission's extensive and far-reaching recommendations on addressing discrimination of certain tribal and ethnic groups, women and children from the national ID registry. These include practical measures to address procedural and social barriers as outlined below:[158]

    - adequately support the Registrar General's department so it can effectively devolve its offices and operations to cover marginalised communities and enhance access to registration services;
    - issue a policy directive prohibiting withholding of birth confirmation records by health institutions and personnel for non-payment of hospital fees resulting in failure to register births essential for obtaining a national ID;
    - to do away with gender-insensitive protocols that impose unjust demands on women as a condition for them to acquire a national ID;
    - amend the birth registration law to include new and emerging or contemporary trends in the family structure, to address changes in traditional family structures so as to enable registration;
    - formulate gender-sensitive policies which take into consideration the gender dimensions of access to documentation, to address gender disparities in registration, as women bear the burden of registering children in the majority of cases;
    - review and develop application procedures and forms that take into account the evolved family structure to allow family members to facilitate acquisition of national documents on behalf of children;

158 See note 139

- use alternative supporting documents, such as health cards and affidavits, to address difficulties faced by women who give birth outside Zimbabwe when registering children where birth confirmation records are not readily available;
- conduct awareness raising campaigns to address cultural impediments which hamper access to documentation, such as the difficulties experienced by women who want to register children in their maiden names due to cultural beliefs that children must carry their father's surnames; and
- educate staff on the intricacies of the local communities they are operating in, to effectively provide the requisite services.

The experiences of other countries can provide instructive lessons on how Zimbabwe's system could address some of the challenges brought about by digital IDs. This would require transparency and accountability as well as the willingness to consult key stakeholders on the part of government; constructive and open civil society engagement with authorities; robust parliamentary oversight; as well as extensive public awareness campaigns on the implications of digital ID on citizens' livelihoods and rights. These efforts, though not exhaustive, will help to ensure a requisite balance between the promotion of digital IDs and the protection of citizens' rights, which is central in building trust between the government and the public in the implementation of the system.

REFERENCES

Amnesty International (2021). Zimbabwe Statelessness crisis traps hundreds of thousands in limbo. *https://www.amnesty.org/en/latest/news/2021/04/zimbabwe-statelessness-crisis-traps-hundreds-of-thousands-in-limbo/*

Atik, J.J. (2017). Digital Identity: Essential Guide. ID4Africa Identity Forum. *https://www.id4africa.com/main/files/Digital_Identity_The_Essential_Guide.pdf*

Centre for Intellectual Property and Information Technology Law. (2020). Report on Narratives on Digital ID in Africa. Strathmore University. *https://cipit.strathmore.edu/wp-content/uploads/2020/11/Report-on-Online-Narratives-on-Digital-ID-in-Africa-copy-optimized.pdf*

Chair, C., & Majama, K (2020). Digital IDs in Zimbabwe: A Case Study. The Engine Room. *https://www.digitalid.theengineroom.org*

Devermont, J. & Harris, M. (2021, June 9). Digital Africa: Leveling Up through Governance and Trade. Center for Strategic and International Studies. *https://www.csis.org/analysis/digital-africa-leveling-through-governance-and-trade*

European Commission (2021). Regulation on a European Approach For Artificial Intelligence. *https://www.politico.eu/wp-content/uploads/2021/04/14/AI-Draft.pdf*

Justice for Children.(2007). Birth Registration of Children in Zimbabwe. *http://archive.kubatana.net/docs/chiyou/jct_birth_registration_0710.pdf*

Human Rights Watch. (2008). *https://www.hrw.org/report/2008/06/09/bullets-each-you/state-sponsored-violence-zimbabwes-march-29-elections*

International Crisis Group. (2017). Zimbabwe's "Military-assisted Transition and Prospects for Recovery. *https://www.crisisgroup.org/africa/southern-africa/zimbabwe/b134-zimbabwes-military-assisted-transition-and-prospects-recovery*

International Telecommunications Union (2018). Digital ID Roadmap Guide. *https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU_eID4D_DIGITAL%20IDENTITY_ROAD_MAP_GUIDE_FINAL_Under%20Review_Until-05-10-2018.pdf*

Manby, B. (2019). Report on Citizenship Law: Zimbabwe, GlobalCIT: European University Institute

Malunga, S. (2019. Zimbabwe-Corruption and Patronage do more than sanctions. Africa Report. *https://www.theafricareport.com/19293/zimbabwe-corruption-and-patronage-do-more-damage-than-sanctions/*

McKinsey Global Institute. (2019). Digital Identification: A key to inclusive growth. *https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#*

Mhike, C. (2020). The Cyber Security and Data Protection Bill Review. *https://www.veritaszim.net/sites/veritas_d/files/Cyber%20Security%20%20Data%20Protection%20Bill%20Commentary.pdf*.

MISA Zimbabwe (2020). Submissions on Cyber Security Bill. *https://zimbabwe.misa.org/2020/06/25/misa-writes-to-parliament-submissions-on-the-cybersecurity-bill/*

MISA Zimbabwe. (2018). Zimbabwe's urgent need for data privacy laws. *http://zimbabwe.misa.org/2018/07/13/zimbabwes-urgent-need-data-privacy-laws/*

Moyo, J. (2019). Excelgate: How Zimbabwe's 2018 Presidential Election Was Stolen, Sapes Books: Harare

Mudede, T., & Machiri, H. (2012 November 26-29). Production of Machine Readable Documents: The Zimbabwean Situation. (Conference Presentation). International Civil Aviation Organisation Regional Seminar on MRTDs, Biometrics and Border Security Conference, Victoria Falls, Zimbabwe. *https://www.icao.int/Meetings/mrtd-Zimbabwe2012/Documents/6-Mudede_Machiri_Zimbabwe-Situation.pdf*

Ndhlovu, G.N. (2019). The Ethnicity of Development? Discourses Shaping Developmental Politics in Rural Matabeleland South, Zimbabwe. *African Journal of Social Work*: AJSW, 9 (1). 35-45

Ojokorotu, V., & Kamidza, R. (2018). Look East Policy: The Case Of Zimbabwe–China Political And Economic Relations Since 2000. *India Quarterly: A Journal of International Affairs*. 74(1), 17-41. *https://doi.org/10.1177/0974928417749642*

Parliament of Zimbabwe. (2021). The Constitution of Zimbabwe. *https://www.parlzim.gov.zw/component/k2/download/1290_da9279a81557040d47c3a2c27012f6e1*

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

Privacy International (2018). A Guide for Policy Engagement on Data Protection: Data Protection Principles. *https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf*

Research and Advocacy Unit. (2008). A Right or a Privilege: Access To Identity and Citizenship in Zimbabwe. *http://citizenshiprightsafrica.org/wp-content/uploads/2016/07/Dube_Zim_Right-or-privilege-Citizenship-Identity-2008.pdf*

Sithigh, D.M., & Siems, M. (2019). The Chinese social credit system: A model for other countries?. European University Institute Department of Law. *https://cadmus.eui.eu/bitstream/handle/1814/60424/LAW_2019_01.pdf?sequence=1&isAllowed=y*

Statista. (2021). Zimbabwe Statistics and Facts. *https://www.statista.com/topics/4353/zimbabwe/*

Rupiya, M. (2011). The Military Factor in Zimbabwe's Political and Electoral Affairs: *https://www.semanticschol:ar.org/paper/The-Military-Factor-in-Zimbabwe%E2%80%99s-Political-%26/7287e99e7347cb686a4b893e24888acb296c1f2a*

Shepard, W. (2019, October 3). What China is really up to in Africa? Forbes. *https://www.forbes.com/sites/wadeshepard/2019/10/03/what-china-is-really-up-to-in-africa/?sh=8ec528559304*

Svantesson, D. (2020). Data Localisation Trends and Challenges: Considerations for the Review of The privacy Guidelines. OECD Digital Economy papers. *https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges_7fbaed62-en;jsessionid=r4z7JOHj_PhNPZf7_8VBO-mx.ip-10-240-5-60*

Thales Group. (2021, April 6). Biometrics: definition, use cases and latest news. *https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics*

The World Bank. (2017). The State of Identification Systems in Africa: Country Briefs. *https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf?sequence=1&isAllowed=y*

The Herald. (2020, November 16). Development Strategy 1 set for today. *https://www.herald.co.zw/development-strategy-1-launch-set-for-today/*

Thornycroft, P. (2002, January 10). Military will not accept Mugabe defeat. The Telegraph. *https://www.telegraph.co.uk/news/worldnews/africaandindianocean/zimbabwe/1381018/Military-will-not-accept-Mugabe-defeat.html*

Zimbabwe Human Rights Commission. (2020). Report on National Inquiry on Access to Documentation in Zimbabwe. *http://citizenshiprightsafrica.org/wp-content/uploads/2016/07/Dube_Zim_Right-or-privilege-Citizenship-Identity-2008.pdf*

United Nations Development Group. (2017). Data Privacy, Ethics And Protection Guidance Note On Big Data For Achievement Of The 2030 Agenda. *https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf*

World Bank (2021 June 10) Zimbabwe Overview. *https://www.worldbank.org/en/country/zimbabwe/overview*

World Population Review (2021). Zimbabwe Population. *https://worldpopulationreview.com/countries/zimbabwe-population*

ANNEX 1

OVERVIEW OF EVALUATION FRAMEWORK

In 2019, the Centre for Internet and Society (CIS) published "Governing ID: Principles for Evaluation" ("Evaluation Framework"), which set out a framework for the evaluation of digital identity. The Evaluation Framework should be read alongside CIS' glossary of 'Core Concepts and Processes' that explains different principles such as identification, authentication, foundational and functional identity systems, that are present in any Digital ID system. Early draft frameworks were published in the lead up to RightCon 2019 held in Tunisia and were discussed at an event organized by Omidyar Network titled "Holding ID Issuers Accountable, What Works?"

The impetus for this document came from Clause 16.9 of the UN Sustainable Development goal, "By 2030, provide legal identity for all, including birth registration". Thus, countries across the world have begun implementing new, foundational, digital identification systems ("Digital ID"), or begun to modernize their existing ID programs.

The history of digital ID programmes in countries such as India, Kenya, Estonia, Jamaica, and the U.K. demonstrated the different concerns associated with privacy, surveillance, exclusion, and mission creep. CIS felt that there was urgent need for further analysis and discussion into the appropriate (and inappropriate) uses of digital ID systems. Through research, we realised that the use of a Digital ID system is inextricably linked to the governance structure and fundamental attributes of the Digital ID system. Hence, a use analysis of Digital ID systems is best accomplished through an evaluation framework that provides principles against which Digital ID may be evaluated.

Consequently, the Evaluation Framework lays out a series of tests that can be used across jurisdictions to assess the legitimacy and governance of Digital ID. CIS selected three sets of tests – the Rule of Law tests, Rights-based tests, and Risks-based tests – to form the bedrock of the Evaluation Framework for Digital ID. CIS adopted the definition of 'digital identity' provided by David Birch, as a "system where identification (the process of establishing information about an individual), authentication (the process of asserting an identity previously established during identification) and authorisation (the process of determining what actions may be performed or services accessed on the basis of the asserted and authenticated identity) are all performed digitally". Such a definition departs from the ID4D Practitioner's Guide that defines authorisation from the lens of eligibility, i.e. the process of determining whether a person is 'authorised' or 'eligible'.

In coming up with these tests, CIS adopted a first principles approach, drawing from methodologies used in documents such as the international Necessary & Proportionate Principles on the application of human rights to communication surveillance, the OECD Privacy Guidelines, and international scholarship on harms based approaches.

RULE OF LAW TESTS

Digital ID systems per se involve a vast collection of personal and sensitive personal data that infringe the privacy of individuals. Any such restriction on fundamental rights must be legal, backed by a legitimate aim, narrowly tailored in scope and application, accountable, and prevent mission creep. Hence, the Rule of Law tests evaluate whether a rule of law framework exists to govern the use of Digital ID and ensure sufficient deliberation before a Digital ID system is implemented for public and private actors. These tests ask six questions about:

1) **Legislative mandate** – whether the Digital ID project is backed by a validly enacted law, and whether the law amounts to excessive delegation.

2) **Legitimate aim** – whether the law has a validly defined legitimate aim.

3) **Actors and purpose** – whether the law clearly specifies the actors who use digital ID and the purposes for which the Digital ID is used.

4) **Grievance redress** – whether the law provides for adequate redressal mechanisms against actors who use the Digital ID and govern its use.

5) **Accountability** – whether there are adequate systems of accountability for all the (public and private) actors and users in the Digital ID system.

6) **Mission creep** – whether there is a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of Digital ID.

RIGHTS-BASED TESTS

Criticism of Digital ID systems focus on their violations of privacy – whether through the mandatory collection of sensitive personal data, risk of surveillance and profiling, or the lack of robust access control mechanisms – and the risk of exclusion. Hence, the Rights-based tests put forth certain rights-based principles, such as necessity and proportionality, data minimisation, access control, exclusion, and mandatory use that should be used to evaluate the extent to which the rights of citizens are being infringed through the use of Digital ID systems.

These tests ask five questions about:

1) **Necessity and proportionality** – whether the privacy violations arising from the use of Digital ID necessary and proportionate to achieve the legitimate aim.

2) **Data minimisation** – whether there are clear limitations on what data may be collected, how it may be processed, and how long it is retained for, during the use of Digital ID.

3) **Access control** – how is access by state and private actors to personal and sensitive personal data controlled through the law.

4) **Exclusion** – whether there are adequate mechanisms to ensure that the adoption of Digital ID does not exclude citizens/residents or restrict their access to benefits and services.

5) **Mandatory use** – whether there are valid legal grounds to justify the mandatory nature of Digital ID, if any.

RISK-BASED TESTS

A rights-based constitutional approach to evaluating Digital ID is necessary, but not sufficient, to ensure a well-functioning Digital ID system. Regulation of Digital ID must be sensitive to the different types of harms caused by its uses (such as privacy harms, exclusion harms, and discriminatory harms), the severity and likelihood of the harm, and must build in mitigation mechanisms to reduce the probability or impact of the harm. Although most countries do not perform such risk-based tests, CIS hopes that by incorporating these tests into the Evaluation Framework, governments will have a more realistic picture of the harms that are likely to occur in a Digital ID system and take appropriate steps to reduce the risk of the same. These tests ask five questions about:

1) **Risk assessment** – whether decisions regarding the legitimacy of uses, benefits of using Digital ID, and their impact on individual rights is informed by risk assessment.

2) **Differential risk approach** – whether the law adopts a differentiated approach to governing uses of Digital ID (such as per se harmful, per se not harmful, and sensitive), based on the risk factors.

3) **Proportionality** – whether the governance framework in the Digital ID law is proportional to the likelihood and severity of the possible risks of its use.

4) **Response to risks** – given certain demonstrably high risks from the use of Digital ID, whether the law has built in mitigatory mechanisms to restrict such use.

Using the Evaluation Framework, CIS published case studies on the use of Digital ID for the delivery of welfare, for verification, and in the health care sector. Country specific case studies were carried out for Estonia's e-Identity program, India's e-KYC framework, India's Unique Identity (Aadhaar) programme, and Kenya's Huduma Namba programme.

The eventual aim of the Evaluation Framework is to evolve these three tests into a set of best practices that can be used by policymakers when they create and implement Digital ID systems; provide guidance to civil society to evaluate the functioning of a Digital ID system; and highlight questions for further research on the subject. Through this project, in collaboration with RIA, we hope to fulfil some of these goals. ■