Digital Identity in Lesotho

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

RESEARCH & WRITING
Nthabiseng Pule

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 Lesotho

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 Lesotho

By Nthabiseng Pule, RIA

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 systems in Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa,

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.

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 Lesotho case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Nthabiseng Pule, RIA. 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 Nthabiseng Pule, RIA 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

In 2011, the government of Lesotho passed the National Identity Cards Act 2011, which paved the way for establishing a national digital identity register and issuing national identity cards (ID cards). In 2013, the register, managed by the Department of National Identity and Civil Registry in the Ministry of Home Affairs, was established based on this law. The Act requires that all eligible persons use the national ID card issued in terms of this law to "access all services". It is not clear if and how the mandated use of the government's digital ID, to the exclusion of other means of identification, has affected citizens.

This research explores the governance of the digital ID system established under the National Identity Cards Act 2011. It does so by applying the Centre for Internet and Society's "Governing ID: Principles for Evaluation" framework. In general terms, the framework applies three categories of tests: a) rule of law tests, b) rights-based tests and c) risk-based tests.

Findings suggest that, to a limited extent, digital ID governance in Lesotho passes some of the rule of law tests, in that it is backed by an act of parliament, even though within the Act itself there are clauses that do not pass the quality of law test; there is also a wide scope of discretion given to the minister. On the rights-based tests, Lesotho does not pass the test because the Act allows for the collection of personal data, including biometrics, and sharing of the same by several actors, while safeguards against abuse and cybersecurity threats are insufficient. On risk-based tests, the governance system in Lesotho fails a number of tests. The most concerning are risks of privacy harms, exclusion harms, mission creep and indiscriminate data sharing. The report ends with recommendations on how the government of Lesotho and other stakeholders may improve the digital ID implementation and governance in the country to minimise the identified risks while maximising the potential benefits of digital ID.

ACRONYMS AND ABBREVIATIONS

Act	National Identity Cards Act, 2011
CIS	Centre for Internet and Society
GDPR	The General Data Protection Regulation (EU) 2016/679
GNI	Gross National Income `
ID	Identity (document)
LDC	Least Developed Country
MoHA	Ministry of Home Affairs
NICR	Department of National Identity and Civil Registry
NISSA	National Information System for Social Assistance
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNHCR	United Nations High Commissioner for Refugees
USSD	Unstructured Supplementary Service Data

CONTENTS

INTRODUCTION

Lesotho launched a foundational digital identification platform and a digital identity card in 2013 based on the National Identity Cards Act, 2011[9] (hereafter referred to as the Act). A foundational digital identification platform is a general-purpose digital system designed to serve multiple identity functions and applications (or identity use cases); other digital identities are built on top of it.[10] A foundational digital system is built by the state to support national development and is designed for use across several sectors.[11] It provides the basis for functional digital identities such as a driver's licence, voter's card, health record or bank card.[6] The Government of Lesotho determined as far back as 2007 that there was a need for a trusted citizen identification system that would provide each citizen with a unique identity number to support several developmental objectives for which the availability of a trusted identification regime was key.[12] It is generally reported that by 2020, over 85% of the eligible 1.2 million citizens had registered and obtained an ID card.[13]

The Act's objective is to provide for the establishment of the National Identity Register (register) and the issuance of national identity cards (national ID card/ ID card).[14] In this report, the term "digital ID" refers to the digital identity data in the register. The data in the register facilitates the production of national ID cards. The Act makes it compulsory for all eligible persons to use the national identity card to access services.[15] Eligible persons are those aged 16 and older, who are either citizens or non-citizens with an indefinite residence permit.[16]

This report evaluates the governance of the ID system and identifies potential areas for improvement. The report first presents the digital ID context in Lesotho. Next, the rule of law principles and tests, rights-based principles and tests, and risk-based principles and tests are evaluated, followed by the conclusion. These

9 National Identity Cards Act 2011 (LSO)

10 *https://lei.info/portal/wp-content/uploads/2020/04/whitepaper_lei.pdf*

11 *https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf?sequence=1&isAllowed=y*

12 *https://www.centralbank.org.ls/images/Publications/Research/Reports/MonthlyEconomicReviews/2008/Economic_Review_June_2008.pdf*

13 *https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center*

14 National Identity Cards Act 2011 (LSO), s.3

15 National Identity Cards Act 2011 (LSO), s.16

16 National Identity Cards Act 2011 (LSO), s.13

tests are based on CIS' *Governing ID: A Framework for Evaluation of Digital Identity*.[17]

1.1 DIGITAL ID CONTEXT IN LESOTHO

Lesotho is a mountainous country, landlocked within South Africa. It has just over 2 million inhabitants, of which 57.9% reside in rural areas.[18] Designated by the UN as a least developed country (LDC),[19] Lesotho has a gross national income (GNI) per capita of USD 1 296.[20] Based on the extended definition of unemployment, the 2018 labour force survey showed a national unemployment rate of 38.3%.[12] The highest percentage of unemployment is in the rural areas.[12] According to the Bureau of Statistics,[21] close to half of the population (49.7%) live below the official poverty line. A significant percentage of citizens are migrant workers in South Africa, and 60% of households in the country receive remittances from South Africa every month.[22]

Lesotho's parliament passed the National Identity Cards Act in 2011 and it was published in the Government Gazette on 21 March 2011.[23] The national ID system, which is based on the Act, was launched on 3 June 2013.[24] Prior to the Act, Lesotho did not have a national identification regime that imposed a single method of identification of citizens and residents. Passports were commonly used for both travel and identification, but this became a challenge when there were years of backlog in the issuance of passports.[25] Passports are no longer widely accepted as a means of identification for accessing services in Lesotho.[26] Functional IDs, such as drivers' licences or electoral cards, which were once used, are also no longer accepted.

For a long time, some form of identification has been a condition of employment in the country. Therefore, delays in the issuance of passports resulted in people

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

18 Bureau of Statistics. (2021). 2019 Labour force survey (LFS) report. Statistical Report No.5 of 2021. Retrieved April 27, 2021 from *http://www.bos.gov.ls/Publications.htm*

19 *https://www.un.org/development/desa/dpad/least-developed-country-category.html*

20 *https://unctad.org/topic/least-developed-countries/list*

21 *http://www.bos.gov.ls/*

22 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

23 National Identity Cards Act 2011 (LSO)

24 *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

25 *https://www.centralbank.org.ls/images/Publications/Research/Reports/MonthlyEconomicReviews/2008/Economic_Review_June_2008.pdf*

26 *https://www.lesotho-diocesan-association.org/lesotho-finally-introduces-national-id/*

losing job opportunities, mainly in the garment manufacturing sector in Lesotho, and the mining sector in South Africa, according to a report by the Central Bank.[27] The report further indicates that the government had identified the lack of a trusted national identification system in Lesotho as an impediment to implementing several policy measures, such as financial inclusion, managing the risk of money laundering, and combating the financing of terrorism, among other things.[13]

The Act affects every aspect of life where identification is required. Section 16 mandates that the identity card issued in terms of the Act be used for identification when accessing all services in the country that require an identification document.[28] Section 12(1) stipulates that the identity card must have the following information of the bearer: full names and surname, nationality, date of birth, image, signature, thumbprint, date and place of issue, date of expiry, identity card control number, national identity number, the name of the issuing authority and any other information that the minister may prescribe.[29] In addition to details on the card, the Act prescribes information that must be on the identity card chip. Section 12(2) requires the chip to contain the following information on the bearer of the card: place of birth, marital status, prints of the right and left index fingers, prints of the right and left middle fingers, residential address, next of kin, occupation and "any other information that the minister may prescribe".[30] No documentation could be found that explains the reasons behind the requirement to capture changing information such as marital status, residential address and occupation.

By the end of 2020, 85% of eligible citizens had been enrolled into the ID system and had obtained an identity card.[31] There are various reasons for the 15% gap in registrations, but the lack of supporting documents such as a birth certificate is the one that the local media has reported on.[32] To avoid excluding some sectors of society, some entities do not strictly apply the Act, as they allow for other forms of identification. For example, the Independent Electoral Commission provides the option of a passport or a sworn affidavit in lieu of an ID when enrolling to register as a voter.[33] The identity card is required to access essential

27 *https://www.centralbank.org.ls/images/Publications/Research/Reports/MonthlyEconomicReviews/2008/Economic_Review_June_2008.pdf*

28 National Identity Cards Act 2011, (LSO) s.16

29 National Identity Cards Act 2011, (LSO) s.12(1)

30 National Identity Cards Act 2011, (LSO) s.12(2)

31 *https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center*

32 *https://lestimes.com/ids-for-all-basotho-mission-impossible/*

33 *http://www.iec.org.ls/requirements-in-registration/*

services where a person is required to provide identification. Examples include applying for a passport,[34] a driver's licence or receiving government welfare benefits.[15] Lesotho's Money Laundering and Proceeds of Crime Act 4 of 2008 mandates accountable institutions to verify the identity of their customers.[35] Such verification, commonly known as know-your-customer (KYC), can only be done through the Lesotho national identity card issued in compliance with the Act.[36] In May 2021, Lesotho's parliament passed the Communications (Subscriber Identity Module and Mobile Device Registration) Regulations 2021,[37], which mandates the registration of SIM cards and mobile devices Specifically, the regulations require registrants to present their national identification number or document to the mobile network operator (licensee) or its agent for the purpose of registering a device or a SIM card.[38]

The Act provides for the authorisation of several actors to access data in the register. Section 6 deals with the conditions and authorisation to access information in the register.[39] It indicates that the director may grant access to a third party if so approved by the minister; it also provides for access to enable a person to view or correct information held about them. Third parties are granted access to the register upon signing a Memorandum of Understanding (MoU) with the Ministry of Home Affairs (MoHA) and paying a fee, according to officials from the Department of National Identity and Civil Registry (NICR). According to NICR officials, a few insurance companies, the only credit bureau in the country, mobile network operators and banks are already connecting to the system for data validation.

1.2 METHODOLOGY

The findings in this report are based on a desktop study and discussions with MoHA officials. Documents reviewed include relevant laws, various reports and other online content such as newspapers, blogs and videos. Discussions with the MoHA were meant to find out about the existence of any regulations and other instruments that support the implementation of the Act. A significant limitation of

34 Lesotho Passports and Travel Documents Act 2018. s.10(2)(c)(ii). *http://citizenshiprightsafrica.org/wp-content/uploads/2020/09/Lesotho-Passports-and-Travel-Documents-Act-2018.pdf*

35 Money Laundering and Proceeds of Crime Act 2008 (LSO), Section 16 (1)(b) *https://fiu.org.ls/legislation/Money_laundering_&_Proceeds_of_Crime_Act.pdf*

36 Money Laundering and Proceeds of Crime Act 2008 (LSO), Section 16 (1)(b)

37 Communications (Subscriber Identity Module and Mobile Device Registration) Regulations 2021

38 Communications (Subscriber Identity Module and Mobile Device Registration) Regulations 2021 s. 21

39 National Identity Cards Act 2011, (LSO) s.6

the study is that it was impossible for the researcher to obtain reports relating to project planning between 2011 and 2013; it was also not possible to obtain copies of agreements between MoHA and actors that are granted access to data in the register. This made it impossible to assess the extent to which those instruments minimise personal data privacy risks.

EVOLUTION OF THE LESOTHO NATIONAL IDENTITY SYSTEM

The Lesotho digital ID system is based on civil registrations (of births, deaths, marriages) and consists of a central database, the national identity register (the NICR also uses the term "population database" to describe the register (Raboletse, 2019)). According to Raboletse, the database is connected to the Birth and Death Registration System, the Marriage and Divorce Registration System, the ID Card System, the ePassport System, the eBorder Control System, the Enquiries, and Reports, Administration Management System, as well as the Stock Control System.[40]

Prior to 2013, when the NICR launched the new ID system, Lesotho did not have a digital ID system. No data was taken from any existing system to populate the new database, because the most obvious one was passport data since passports were the most common form of identification. However, there were concerns about the reliability of passport data because some people held multiple passports under different names and particulars.[41] The NICR decided to not register people based on existing identification documents. Instead, each applicant was required to first apply for a birth certificate issued through the new system.[42] Original birth certificates or other proof of birth (such as a baptismal certificate) were not to be used to apply for an ID; instead, they were used as part of the supporting documents for birth registration[43] to minimise the risk of fraudulent registrations.[44]

The system is administered by the NICR, located in the MoHA. It is responsible for civil registrations such as births, deaths and marriages, and also issues passports. [45] The NICR has the authority to grant access to other parties as provided for in Section 6 of the Act.[46] The system uses an application programming interface (API) to enable remote access to third parties.[47] This

40 *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

41 *https://saiia.org.za/research/african-integration-what-do-new-national-ids-in-lesotho-and-south-africa-mean/*

42 *https://www.youtube.com/watch?v=kDMvVQUGETg*

43 *https://lestimes.com/molapo-eases-id-requirements/*

44 *https://lestimes.com/ids-for-all-basotho-mission-impossible/*

45 *https://getinthepicture.org/sites/default/files/resources/ID4D-country-profiles-report-final.pdf*

46 National Identity Cards Act 2011, s. 6(2)

47 *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

integration interfaces with the Independent Electoral Commission, the Credit Bureau (Compuscan), law enforcement agencies, insurance companies, financial sector institutions (banks and digital payments service providers) and government departments.[48]

The ID cards issued by the NICR do not have a chip; instead, they have a two-dimensional barcode that contains vital information, fingerprints and a photo (Raboletsi, 2019). One side of the card is printed with the registrant's details for identification offline; particulars on the card include name, date of birth and a photo, while the other side has a two-dimensional computer-readable encoding of the bearer's information.[49] Even though online biometric verification has been successfully piloted for use by migrant workers based in South Africa, there is no evidence of widespread use. Access to the register is provided to various parties, such as credit bureaus, banks and mobile network companies, for customer verification purposes through APIs.[50]

The application of digital ID in daily life is not yet a common phenomenon in Lesotho because digitisation is low. For instance, the Rapid eTrade Readiness Assessment[51] established that, among other things, the use of e-commerce platforms by small firms was limited, and the use of cash on delivery remained prominent; while a few online payment channels existed, their use was limited. Lesotho was ranked 118 out of 152 countries on the UN Conference on Trade and Development (UNCTAD) *Business-to-Consumer Index 2020*,[52] indicating low digital economy readiness. The 2020 UN *E-Government Development Index* (EGDI)[53] ranked Lesotho 136 out of 193 countries; this is another indicator of low digitisation because the EGDI assesses the provision of online services, telecommunication connectivity and human capacity by governments.

The 2020 *Lesotho Digital Diagnostic* report established that the Lesotho ID system (the digital ID) needed to be improved to increase the ability of third parties to conduct biometric authentication.[54] The report also indicated several areas for improvement on the existing legal framework to support data sharing, ensure

48 *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

49 Raboletsi, T. (2019). *The Multiplier Effect of Digital ID and Financial Inclusion in Lesotho*. *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf.*

50 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

51 *https://unctad.org/system/files/official-document/dtlstict2019d8_en.pdf*

52 *https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf*

53 *https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/95-Lesotho/dataYear/2012*

54 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

data minimisation and bolster transparency and accountability. Following is an analysis of the NICA using CIS' Evaluation Framework.

RULE OF LAW PRINCIPLES AND TESTS

3.1 LEGISLATIVE MANDATE

Digital ID is established through Section 3 of the National Identity Cards Act 2011, which reads:

> "(1) There is established a National Identity Register.
>
> (2) The register is established to –
>
> (a) facilitate the maintenance of a record of prescribed personal information about citizens of Lesotho and non-citizens holding an indefinite residence permit of Lesotho;
>
> (b) ensure that the existence of accurate and reliable information about the person referred to in paragraph (a); and
>
> (c) be used for specific purposes permitted or prescribed in terms of this Act or any other law".[55]

Section 12 goes on to describe the information that must be on the card and in the chip and indicates that "the form of the identity card shall be prescribed".[56] The Act provides for the production of an identity card with a chip, but the NICR is issuing cards without a chip. Instead, the card is implemented with what is referred to as a two-dimensional barcode.[57] The law amounts to excessive delegation in so far as paragraph 4(6)(w)[58] permits the minister to prescribe any other information for inclusion in the register. Excessive delegation is also apparent in section paragraph 6(7), which reads:

> "The Minister may prescribe, from time to time, persons who may have access to the Register for prescribed purposes".[59]

Regarding the **legality** test, the Act passes the legality test in some aspects but not others. The purpose of the law is to provide for the establishment of the register and the issuance of National Identity Cards.[60] Section 3 of the Act

55 National Identity Cards Act 2011, (LSO) s.3

56 National Identity Cards Act 2011, (LSO) s.12

57 *https://id4africa.com/2015/presentations/31_Tumelo_Raboletsi.pdf*

58 National Identity Cards Act 2011, (LSO) s.4 (6) (w)

59 National Identity Cards Act 2011, (LSO) s.6 (7)

60 The Parliament of Lesotho. (2011). Statement of Objects and Reasons of the National Identity Cards Act, 2011. Government Notice No. 21 OF 2011

establishes the register; Section 4 provides for the registration of persons and the data to be collected; Section 5 mandates the assignment of a unique number known as the National Identity Number to a person who registers and that the number shall comply with prescribed requirements; Section 6 provides for access to data in the register by third parties and by persons who want to access their own data; Section 7 deals with the responsibility of the director to ensure the accuracy and quality of data; it also provides for a person about whom data is held to update their data as their life circumstances force changes in the data held about them in the register.[61]

The socio-political reasons for implementing the register are not provided in the Act. Instead, the socio-political reasons for it can be picked up from statements made by government officials such as the director and minister[14] addressing media.[62] From these sources, it can be concluded that the purpose of the national identity card is to facilitate the delivery of services to citizens. In a blog post, Ort and Rabeletse (Principal Secretary, MoHA) indicate that among the benefits realised through the implementation of the register is having identity verification services for both the private sector and public sector, which is key for the delivery of social assistance services and improving access to financial services.[63]

In relation to the **quality of law** test**,** the Act does not meet the foreseeability standard because some clauses are unclear or introduce uncertainty. For example, paragraph 3(2)(c) on the purpose of establishing the register is not clear. Apart from that, paragraphs 4(6)(w), 6(7), 12(1)(l) and 12(2)(g) allow the minister to introduce things that are not currently in the Act. Furthermore, the Act is written in English and there are no translations to Sesotho and other languages spoken in the country; citizens who are fluent in the English language are a minority.[64] Sesotho is the native language spoken by about 90% of the population. There are three or four minority languages: Ndebele/Zulu, Phuthi, and isiXhosa.[65] Chapter 1 Section 3(1) of the 1993 Constitution states that English and Sesotho are the official languages.[66] Furthermore, like most Lesotho laws, the Act is not readily accessible; there are no electronic copies and copies can only be bought from the Government Printing Office located in Maseru. The cost of travel to obtain a copy of the law is high for the average citizen because of the high poverty rate.

With regards to the **clarity and precision** test, the Act is generally clear, though

61 National Identity Cards Act 2011, s. 7

62 *https://lestimes.com/molapo-eases-id-requirements/*

63 *https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center*

64 *https://www.unicef.org/esaro/UNICEF(2016)LanguageandLearning-Lesotho.pdf*

65 *https://www.britannica.com/place/Lesotho*

66 *https://lesotholii.org/ls/legislation/num-act/1993/1*

there are a number of vague clauses as the following instances illustrate. The Act uses the term "prescribed", which is assigned the meaning "prescribed by regulations".[67] Section 3, which describes the purposes of the register, ends with: "... to be used for specific purposes permitted or prescribed in terms of this Act or any other law".[68] In specifying the particulars to be included in the register, the Act lists out the data attributes to be stored and it ends with the clause "any other information that the Minister may prescribe".[69] In addition to this, on access to the register, the last paragraph provides that "The Minister may prescribe, from time to time, persons who may have access to the Register for prescribed purposed"[70]. The Act lists out the information to be printed on the identity card[71] and to be stored the chip embedded in the card and it ends with "... and any other information that the Minister may prescribe".[72] The preceding clauses are areas where regulations[73] envisaged in the Act were supposed to provide clarity. However, such regulations, according to the NICR officials, have not yet been developed. Even though the Act provides for the minister to make these regulations, there is a risk of excessive executive discretion; instead, new features and requirements should follow a legislative process by way of either amendments or a new law.

3.2 LEGITIMATE AIM

The Act does not state the purpose of establishing the digital ID or mandating its universal use for eligible persons.[74] However, it can be deduced from some sections of the Act that one purpose of implementing the digital national identity project was to enable identity verification by actors listed in the Act for the interest of public order, public safety, public health, to detect and prevent fraud as well as to uphold the legitimate interests of the actors.[75] The primary purpose of the Lesotho national identification system is to have a trusted method of identification that provides a unique identification number to every citizen and

67 National Identity Cards Act 2011, s. 2
68 National Identity Cards Act 2011, s. 3 (2)(c)
69 National Identity Cards Act 2011, s. 4(6)(w)
70 National Identity Cards Act 2011, s. 6(w)
71 National Identity Cards Act 2011, s.12 (1)(l)
72 National Identity Cards Act 2011, s.12 (2)(g)
73 National Identity Cards Act 2011, s.20
74 National Identity Cards Act 2011, s 16
75 National Identity Cards Act 2011, s.6(2)

resident for universal use in the country.[76] The outcomes of implementing a trusted digital identification system include improved public and private sector efficiency and financial inclusion.[77] In Lesotho, among other things, digital ID is used for access to credit, controlling insurance fraud, implementing the public officers census to remove ghost workers from the payroll, and payment of social grants.[78] Based on these assertions, the conclusion is that the Lesotho digital ID has a legitimate aim.

3.3 DEFINING ACTORS AND PURPOSES

The actors in Lesotho's digital ID ecosystem are the citizens, government departments and agencies, and private businesses. The citizens, as defined in the Lesotho Citizenship Order 1971[79] and non-citizens holding an indefinite Lesotho residence permit, are required to use the identity card for proof of identity.[80] Organisations use the digital ID to verify the identities of individuals for business purposes in order to detect or prevent fraud or to verify the particulars of a person for the purpose of entering into a business contract[81]. The Act provides for access to information in the register by government departments, statutory bodies and private entities involved in public order, public safety and public health as actors who may access the ID data in the register. [82] It also provides for access and use by businesses, in particular those in insurance, banking, provision of credit (e.g. money lending or consumer credit), those leasing property out on credit and the credit bureau.[83] Access by these third parties is meant to enable the performance of contracts with those actors to whom the information refers, to prevent or detect fraud or to protect the legitimate interest of the requesting party to verify the particulars of a person whose information is held in the register.[84]

The Act provides for the minister to prescribe other actors in addition to those

76 *https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center*

77 *https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center*

78 *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

79 Lesotho Citizenship Order 1971 [Lesotho], Order No. 16 of 1971, 1971, available at: *https://www.refworld.org/docid/4c5849ad2.html* [accessed 12 June 2021]

80 National Identity Cards Act 2011, s. 16

81 *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

82 National Identity Cards Act 2011, s.6

83 National Identity Cards Act 2011, s.6(2)

84 National Identity Cards Act 2011, s.6 (2)

explicitly stated in the Act.[85] A category of actors that has been approved by the minister, which is not listed in Section 6 of the Act, is the telecommunications network operators licenced under the Communications Act 2012.[86] These network operators are required by regulations to use the national ID when registering the devices and SIM cards of their customers; they are also required to capture biometric data and verify it against data in the registry.[87] The regulations further mandate network operators to send the data to the Lesotho Communications Authority.

The ID cardholder (or bearer) is an actor about whom information is stored in the register. To obtain an ID, a person must provide information about themselves as prescribed by the Act. The Act requires the register to contain: identity number, full names, nationality, passport number (in the case of a non-citizen), date and place of birth, gender, residential address, postal address (if applicable), telephone number (if applicable), marital status, maiden names, headman, principal chief, occupation, place and address of work (if applicable), names of parents, names of next of kin, relation to next of kin, contact details of next of kin, a photograph and fingerprints of the person (if the person has reached the age of 16).[88] While the digital ID is meant to be multipurpose, the information collected is excessive. For example, information collected relating to next of kin, occupation, principal chief and headman is unnecessary.

Since the national identity card is the only method of identification for all eligible persons, it follows that government and the private sector are required to only accept the national ID card for verification of a person's identity. As indicated earlier, the Act makes provision for a third party such as a government agency, credit bureau or network operator to access digital IDs in the register. According to the World Bank Group, a generic API has been developed to provide a mechanism for entities that need access to connect to the register.[89] The generic nature of the API makes it possible for a third party to have access to more information than is strictly necessary and it is not clear how this risk is managed.

To conclude, the law does not provide for a purpose limitation since the Act states that the register may "... be used for specific purposes permitted or

85 National Identity Cards Act 2011, s6(7)

86 Communications Act 2012, s.19

87 Communications (Subscriber Identity Module and Mobile Device Registration) Regulations 2021 s.2

88 National Identity Cards Act 2011, s.4

89 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

prescribed in terms of this Act or other law",[90] which offers unlimited possibilities on what the digital ID system may be used for. The Act also gives a lot of leeway to the responsible minister to specify new actors or information that may be stored in the register to facilitate uses of the digital ID that were not initially envisaged when the law was passed.

3.4 REDRESSAL MECHANISM

The Act does not provide a clear complaints mechanism beyond granting a person whose information is held in the register the right to request the director to correct errors, as provided for in Section 6 paragraphs 5 and 6, which read:

> "(5) A person who has been given access to his or her information may request that the Director correct inaccurate or outdated information.
>
> (6) A person who has requested that his or her information be corrected shall provide credible evidence of the updated information which shall be verified by the Director in accordance with this Act".[91]

The procedure for the correction of errors is onerous and may result in errors not being rectified. In the case of complaints not relating to the correction of information, such as delays in the issuing of documents, there are no provisions in the Act to deal with such situations. In such situations, according to the NICR officials, the applicant has to seek remedies through the hierarchy of the MoHA, failing which the complainant may seek recourse through the courts of law or the Office of the Ombudsman. There have been complaints about applicants being denied a national identity card for frivolous reasons despite being eligible.[92] In 2013 there were several complaints from people being turned away because they could not obtain the required supporting documentation until rules were relaxed.[93]

User notification is not provided for in the Act; there is no requirement in the Act for a person whose data is in the register to be notified when their data is shared with external parties, or when external parties access the register for verification, or in the case of a breach. The Data Protection Act 2011 gives data subjects a right to request information about their personal data, including information on third

90 National Identity Cards Act 2011, s.6(5)-(6)

91 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

92 *https://lesotholii.org/ls/judgment/high-court/2014/30/*

93 *https://lestimes.com/molapo-eases-id-requirements/*

parties that may have been given access to the data.[94] However, a data protection regulatory body has not been established and therefore there is no enforcement of this law.

The Act is silent on the question of disclosure in the event of a data breach. However, disclosures following a data breach are addressed by the Data Protection Act 2011, which requires the relevant actor to notify the affected person as soon as is reasonably practicable.[95] The Data Protection Act includes a provision for circumstances under which the disclosure of a breach may be delayed;[96] it also provides for how a notification may be made.[97] Redress mechanisms using the Data Protection Act are, however, not implementable because the Data Protection Commission, which is envisaged in the Data Protection Act, has not been established.[98]

Access and corrections are accommodated in the Act. It provides for the person about whom data is held to have access, provided they give sufficient proof of their identity to the director, and they have paid a prescribed fee; a person who has been granted access to their information may request the director to correct inaccurate or outdated information.[99] While there is no documentary evidence that this has happened, it seems possible for the director to refuse a request for corrections if unable to verify the new information, in terms of paragraph 6(6).[100] A person may also notify the director if they notice an error in the information held about them in the register[101] While paragraph 4(b) indicates that a person has to pay a fee in order to be allowed access to data held on them, according to NICR officials the fees have not yet been prescribed.

According to officials of the MoHA, the Act does not provide avenues for redress in the case of unresolved grievances. Grievances against the director or the minister in the administration of the Act have been resolved by the courts of law in the past, as that is the only available legal option. An example is the case of Advocate Zwelakhe Mda, who in 2014 was denied an identity card by the minister,

94 Data Protection Act 2011 (LSO). s. 26

95 Data Protection Act 2011 (LSO) s. 23(1)(b) & s.23(2).

96 Data Protection Act 2011 (LSO) 23(3)

97 Data Protection Act 2011 (LSO) 23(4)-(6)

98 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

99 National Identity Act 2011 (LSO) s. 6(3) - (5)

100 National Identity Act 2011 (LSO) s. 6(6)

101 National Identity Cards Act 2011 (LSO) s. 8(3)

who alleged that Advocate Mda was not a citizen of Lesotho.[102] In this case, the Constitutional Court ruled that based on his birth certificate, Advocate Mda was a citizen and eligible to be issued with an ID.[103] However, the legal route is costly and few people can afford it.

3.5 ACCOUNTABILITY

The Act does not include any regulatory oversight functions over the register and the external actors who access the register. The NICR is a department within the MoHA. According to ministry officials, the Office of Integrity and Quality Assurance has been established within the Ministry to ensure that business processes are followed as required by law. However, there are no regulations. The register is said to operate in alignment with the General Data Protection Regulation (EU) 2016/679 (GDPR), but no audits of the ministry's GDPR compliance have been published.[104]

Administratively, there is no separation of functions. The NIRC is both in charge of data storage, and the authorisation of third parties such as government agencies, banks and network operators. The relationship between the NIRC and the agencies accessing data is governed by means of a MoU and non-disclosure agreements (NDAs), according to ministry officials and the World Bank.[105] The NDAs and the MoUs are not made public. However, the NDA is meant to ensure that parties with whom data is shared do not share it outside the agreed parameters. An MoU or NDA may provide safeguards against abuse. However, they do not obviate the need for a regulatory framework and functional separation. Currently, the NICR acts as an administrator of the register, a regulator who authorises other actors to access the register, and is also involved in enrolments.

3.6 MISSION CREEP

The first factor that makes the digital ID system in Lesotho vulnerable to mission creep is the clause that allows the register to *"... be used for specific purposes permitted or prescribed in this Act or any other law."*[106] This clause is problematic because "any other law" allows for infinite possibilities without seeking a new

102 *https://lestimes.com/mda-wins-citizenship-battle/*

103 *https://lesotholii.org/ls/judgment/high-court/2014/30/*

104 *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

105 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

106 National Identity Act 2011, s 3(2)(b)

mandate from the legislature. Another risk of mission creep results from the fact that the Act gives the minister powers to "prescribe, from time to time, persons who may have access to the Registers for prescribed purpose ".[107] A more definitive prescription would provide certainty about which actors may have access. In addition to enabling the minister to add new actors at will, the Act also gives the minister the powers to specify additional information that may be collected and stored[108] without parliamentary or judicial scrutiny. Therefore, it is possible for the register to extend its mandate to accommodate new actors and their information needs even if such actors are not directly related to the register's purpose of existence, for instance, to increase revenue. Furthermore, the register has developed a generic API for identity authentication and verification but, according to the NICR, there are no regulations for data sharing. The implementation of digital ID without following purpose limitation principles or putting in place procedural safeguards is a cause concern.

Legislative and judicial oversight mechanisms, beyond adherence to the Public Financial Management Act[109] and annual audits by the Office of the Auditor General,[110] do not exist. The Auditor General performs financial audits and may not always pick up a mission creep because the Act gives the minister excessive powers. The lack of a sound governance system was also highlighted in the World Bank Group's *Lesotho Digital Economy Diagnostic Report.*[111] Section 18 (Purpose specification and further processing limitation) of the Data Protection Act 2011 provides controls against mission creep but is not being adhered to.

107 National Identity Act 2011, s.6(7)

108 National Identity Act 2011, s. 4(w)

109 *http://www.finance.gov.ls/documents/laws%20and%20regulations/PFMA%20Act%202011.pdf*

110 Constitution 1993. (LSO). s. 117

111 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

RIGHTS-BASED PRINCIPLES AND TESTS

4.1 NECESSITY AND PROPORTIONALITY

The Act makes acquiring a national identity card mandatory,[112] but does not make it a criminal offence not to have a national identity card. However, a person will not be able to participate meaningfully in the economy without a national identity card, because regulated entities such as mobile network operators, banks and insurance companies are required by other laws and regulations to accept only the national identity card for identification. Examples of the laws and regulations that the private sector must comply with are the Communications (Subscriber Identity Module and Mobile Device Registration) Regulations, 2021, which obliges mobile device users to register SIM cards and mobile devices,[113] *and* the Money Laundering and Proceeds of Crime Act 2008.[114]

In terms of **suitability**, the government did not need to make enrolment and the use of the national ID card mandatory. Instead, the Act should have included a provision that permits a risk-based approach, whereby people may use other forms of identification depending on the use-case. For example, for government grant recipients, the government has to control fraud and prevent double-dipping. In the case of social grants, some of the recipients are children under the age of sixteen who, in terms of section 13 of the National Identity Cards Act 2011, are not eligible to apply for an ID.[115] The World Bank Group (2021)[116] and Kampong *et al*. (n.d.)[117] have identified the lack of specific ID cards for government grant recipients as a challenge afflicting the social protection payment programmes in

112 National Identity Act 2011 (LSO) s.16

113 Communications (Subscriber Identity Module and Mobile Device Registration) Regulations. (LSO). s.20 - 23

114 Money Laundering and Proceeds of Crime Act 2008 (LSO), Section 16 (1)(b)

115 National Identity Card Act 2011, LSO s. 13

116 *https://documents1.worldbank.org/curated/en/996831624982907050/pdf/Lesotho-Social-Protection-Programs-and-Systems-Review.pdf*

117 *https://olc.worldbank.org/sites/default/files/6.%20Alternative%20Payment%20Systems%20-%20Experiences%20from%20Lesotho,%20Nepal%20and%20Pakistan%20_0.pdf*

Lesotho. Due to the HIV pandemic, there are several child-headed households[118] in Lesotho and those children are eligible for support under the Lesotho Child Grants Programme (CGP); registration requires a birth certificate and not an ID.[119] Since the Ministry of Social Welfare, which is responsible for the grants programme, is already registering grant recipients in the National Information System for Social Assistance (NISSA),[120] it could extend NISSA's functionality to include the issuance of digital IDs specifically for grant recipients. Such an ID would not have to be contingent on having the digital ID issued in terms of the National Identity Cards Acts 2011.

There was a **necessity** for a trusted means of identification in 2011 when the National Identity Cards Acts 2011 was passed. The Act paved the way for the launch of the ID card system in 2013.[121] Passports were commonly accepted identification documents, but for several years starting in the early 2000s, there was a backlog in the issuing of passports.[122] Before the Act came into being, passports, driver's licences and election cards were used for identification, but these were criticised as being unreliable means of identification.[72] There were claims that passports were easy to obtain fraudulently and therefore could not be trusted identification documents.[123] The Lesotho government sought to address this problem when it passed the Lesotho Passports and Travel Documents Act 2018 according to its statement of objects:

> "The Bill provides for the establishment of a biometric system whereby the biometric data of the applicants is captured for both identification and verification purposes. This process helps to curb multiple applications by one person".[124]

118 *https://www.thepost.co.ls/news/the-child-headed-families-in-lesotho/*

119 *https://ipcig.org/pub/eng/OP281_The_Impacts_of_the_Child_Grants_Programme_in_Lesotho.pdf*

120 *https://www.gov.ls/nissa-enumeration-launched/*

121 *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

122 *https://www.centralbank.org.ls/images/Publications/Research/Reports/MonthlyEconomicReviews/2008/Economic_Review_June_2008.pdf*

123 SAIIA. (2023, July). *African integration: what do new national IDs in Lesotho and South Africa mean? https://saiia.org.za/research/african-integration-what-do-new-national-ids-in-lesotho-and-south-africa-mean/*

124 *http://citizenshiprightsafrica.org/wp-content/uploads/2020/09/Lesotho-Passports-and-Travel-Documents-Act-2018.pdf*

4.2 DATA MINIMISATION

The Act mandates the director to collect data on several attributes for storage in the register and prescribes the data that must be included.[125] The following particulars of eligible persons are to be included in the register: identity number, full names and surname, nationality, passport number in the case of non-citizens, date and place of birth, residential address, postal address (if applicable), telephone number (if applicable), marital status, maiden names, headman, principal chief, occupation, workplace (if any), address of workplace (if any), names of parents, names of next of kin, a relation of next of kin, address and telephone number of next of kin, a photograph in the case of a person who has attained the age of 16, fingerprints in the case of a person who has attained the age of 16, and "any other information that the minister may prescribe".[126]

The Act prescribes which information must be on the identity card, namely: full names and surname, nationality, date of birth, sex, image of bearer, signature or thumbprint, date and place of issue, expiration date, identity control number, national identity number, marital status, residential address, next of kin, occupation and "any other information that the minister may prescribe".[127] The Act further prescribes the information to be contained in the chip on the identity card; the chip must store the place of birth of the bearer, marital status, prints of the right and left index fingers and the right and left middle fingers, residential address, next of kin, occupation and "any other information that the Minister may prescribe".[128] Since 2013 when the national ID was launched, it is estimated at least 85% (1.2 million) of eligible citizens had registered births and obtained a national identity card by 2020.[129]

Based on the above, it is clear that the Act was not designed with data minimisation as an essential consideration. It requires at least 23 data attributes to be collected and stored in the register. The World Bank Group noted the lack of data minimisation in its 2020 Lesotho Digital Economy Diagnostic report.[108] Not all of the prescribed information is necessary to have a trusted, foundational identification instrument. Paragraph 8(3) of the Act requires a person to notify the director whenever a change of circumstances affects information recorded about them.[130] Collecting unnecessary data imposes an administrative burden on

125 National Identity Card Act 2011, LSO s. 4

126 National Identity Card Act 2011, LSO s. 4(6)

127 National Identity Card Act 2011, LSO s. 12(1)

128 National Identity Card Act 2011, LSO s. 12(2)

129 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

130 National Identity Cards Act 2011, s.8(3)

the registrant to update their details whenever circumstances change, such as if they move homes, or their designated next of kin dies, or there is a divorce; people change jobs, and every time they do, they are required to notify the director.

There is a risk of increased unlawful surveillance when data such as place of work, telephone number and next of kin become accessible to law enforcement agencies which may be authorised to access information in the register as provided for in paragraph 6(2)(b).[131] The more information about a person - such as their workplace and next of kin and telephone number - third parties have access to, the easier it is to triangulate and locate a person for the purpose of surveillance. Government surveillance is a concern in many countries, including Lesotho.[132] [133]

4.3 ACCESS CONTROL

The Act has provisions for access control. It prohibits an unauthorised person from accessing the register or modifying information in the register.[134] In Section 6, Act the provides that the director, with the approval of the minister, may authorise access to a third party in accordance with instructions of the person to whom the information relates.[135] Section 6 provides for access by a government department, statutory body or private entities in the interest of public order, public safety or public health. A specific provision is made for access by businesses whose activities are in the following categories: insurance, banking, credit provision, property credit provision, and credit bureaus for use in contracts to prevent and detect fraud or to protect the legitimate interest of the requestor.[136]

There are risks of abuse emanating from the fact that the Act allows so many actors to access the data in the register. One risk is the use of data in the register for unlawful surveillance of individuals by government authorities without any safeguards, such as court orders. Another risk is that the actors who are given access to data in the register may use it for seeding other databases unrelated to the legitimate uses for which access was provided. Also concerning is the fact that there is no independent oversight body to ensure that the public interest and the privacy rights of citizens are protected.

131 National Identity Cards Act 2011, s.6(2)(b)

132 *https://www.eff.org/issues/national-ids*

133 *https://lestimes.com/govt-approves-draconian-snooping-law/*

134 National Identity Cards Act 2011, s.6(1)

135 National Identity Cards Act 2011, s.6(2)-(7)

136 National Identity Cards Act 2011, s.6(2)(c)

4.4 EXCLUSIONS

Mandatory use of the national identity card results in the exclusion of some people from accessing services even if they hold an alternative method of identification, as has been mentioned above. The Act prescribes eligibility criteria for a national identity card and has excluded some people, such as refugees. Furthermore, the Act does not provide an alternative means of identification for refugees or for applicants whose citizenship may be questioned by the minister in response to an application to register.

In 2018, the government passed the Lesotho Passports and Travel Documents Act 2018, which explicitly lists the national ID card as one of the application requirements, thus increasing the exclusion problem.[137] As a result of this, vulnerable groups such as refugees and people who have not been able to get birth certificates have been excluded from obtaining passports. The exclusion of refugees has been reported by the UN High Commissioner for Refugees (UNHCR) and in 2019, the UNHCR reported on the plight of refugees and stateless persons in Lesotho due to their exclusion from the national identification regime.[138] According to the report, a refugee and a stateless person could not obtain a travel document to travel to neighbouring countries, because a person is required to have a national ID in order to be issued with a passport, and even though the Lesotho Passports and Travel Documents Act 2018[139] has a refugee passport as a category of passport to be issued to refugees, the National Identity Cards Act does not have a similar provision for refugees. As a result, refugees aged 16 and above are excluded from applying for a travel document.

The National Identity Cards Act does not have a provision for dealing with refugees and stateless persons despite Lesotho being a party to several treaties relating to refugees and statelessness, such as the 1951 Convention Relating to the Status of Refugees[140] and its 1667 Protocol.[141] Section 13 of the Refugee Act 1983[142] stipulates that:

1. Subject to this Act, a person claiming to be a refugee or who has been recognised as a refugee shall be subject to the laws and regulations in force

137 Lesotho Passports and Travel Documents Act 2018. s.10(2)(c)(i). *http://citizenshiprightsafrica.org/wp-content/uploads/2020/09/Lesotho-Passports-and-Travel-Documents-Act-2018.pdf*

138 UNHCR. (2019). *https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=7626&file=EnglishTranslation*

139 Lesotho Passports and Travel Documents Act 2018. s.7(6). *http://citizenshiprightsafrica.org/wp-content/uploads/2020/09/Lesotho-Passports-and-Travel-Documents-Act-2018.pdf*

140 *https://www.unhcr.org/5d9ed32b4*

141 *https://www.unhcr.org/5d9ed32b4*

142 The Refugee Act 1983 (LSO) s.13. *https://www.refworld.org/docid/3ae6b4f024.html*

in Lesotho.

2. Notwithstanding sub-section (1), a refugee shall enjoy the rights and be subject to the duties defined in the 1951 Convention and 1967 Protocol relating to the Status of Refugees and the 1969 OAU Convention governing the specific aspects of refugee problems in Africa.

By mandating the use of the national ID card, the Act introduces a risk of excluding people from participating in the economy. In financial services, a person is required to provide their national identity card for verification as stipulated by the anti-money laundering law. To register a mobile device or SIM card, a person has to provide an identity document.[143] An inability to register a device and a SIM card excludes one from both communication services and financial services (e.g. mobile money and internet banking).

Exclusion due to administrative procedures and decisions involving location, language and cost to obtain an ID is a matter of concern regarding the digital ID in Lesotho. Eligible persons may not have obtained a national identity card due to insurmountable obstacles, including poverty, ill-health, or the lack of required supporting documents, as has happened in the past.[144]

According to ministry officials, the national identity card is provided free of charge.[82] Therefore, this fee is not exclusionary. However, issuing centres are often located in towns, which forces rural dwellers to incur high travel costs that some may not afford. To address the issue of costly travel for people living in remote areas, the MoHA, in collaboration with two other government ministries, has established a mobile registration centre intending to register the remaining 200,000 people.[145]

In terms of accommodating offline and localised verification, the Lesotho digital ID system uses an ID card. The card can be used for authentication offline or online with a scanner, according to NICR officials.[146] The ID card has a photograph of the bearer's face, their names in full, date of birth, nationality, date of issue, expiry date and a signature or fingerprint to enable manual verification.

As mentioned earlier, the NICA does not provide for a grievance redress mechanism. In the absence of redress mechanisms that might speed up

143 Communications (Subscriber Identity Module and Mobile Device Registration) Regulations. (LSO). s.20 - 23

144 *https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center*

145 *https://www.biometricupdate.com/202103/lesotho-national-digital-identity-system-within-200000-of-universal-coverage-saving-public-money*

146 Raboletsi, T. (2019). *The Multiplier Effect of Digital ID and Financial Inclusion in Lesotho https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf*

registration, the lack of alternative means of identification in the Act leads to several exclusion harms. People risk being excluded from services such as mobile network communications and banking; a person may even miss job opportunities outside the country as they cannot obtain a new passport if they do not have a national ID. The old passport was phased out in favour of the e-Passport, which is based on the digital identity.[147]

4.5 MANDATORY USE

The government of Lesotho implemented the digital ID because it was looking for a national identification mechanism that gives every citizen and every eligible resident a unique identification number and is trusted.[148] The government is of the view that the inclusion of biometric data enables verification and authentication of identity efficiently and with high certainty, thus fostering trust in the ID.[149]

Section 16 of the Act that underlies mandatory use is quoted here for emphasis:

> "No person who is eligible to have an identity card shall access all services unless the person produces his or her identity card issued in accordance with this Act."[150]

The Act does not provide reasons for making the use of the digital identity mandatory for access to all services. It does not have a provision that obliges a person to apply to have their details included in the register in which the digital IDs are maintained. Instead, it forces enrolment into the register by mandating the use of the national identity card. The identity card is based on the digital information in the register. The Act does not criminalise non-registration nor the failure to acquire a national identity card. However, as already pointed out, the outcome of non-registration is exclusion from the economy.

The Act does not provide alternative means of identification for those who have not yet obtained a national identity card because they live far away from the issuing centres, an estimated 200,000 individuals. The lack of alternative methods of identification in the Act means that the affected people face exclusion from the economy and from government social assistance programmes.

147 SABC News (2018, June 21) *https://www.youtube.com/watch?v=RWHdNuB4P_4*

148 *https://www.centralbank.org.ls/images/Publications/Research/Reports/MonthlyEconomicReviews/2008/Economic_Review_June_2008.pdf*

149 *http://citizenshiprightsafrica.org/wp-content/uploads/2020/09/Lesotho-Passports-and-Travel-Documents-Act-2018.pdf*

150 National Identity Cards Act 2011 (LSO), s 16

Mandatory use is not suitable for Lesotho for a few reasons. The first is the risk of exclusion: a significant number of eligible people have not been able to register due to logistical challenges, combined with poverty. Furthermore, the Act does not have provisions for addressing the identified needs of a population excluded because they cannot obtain documents such as proof of birth. Digital databases (particularly centralised databases) are inherently vulnerable to cybersecurity threats. In the case of a successful cyber breach, all citizen data, including biometric data, may be stolen and abused to the detriment of the citizens. Rather, citizens should have a choice on whether to enrol or not. Mandatory digital ID threatens civil liberties due to its potential to enable unlawful surveillance of citizens. There are no valid reasons to make the use of the Lesotho national identity card mandatory and the only means of identification for all services.

RISK-BASED PRINCIPLES AND TESTS

5.1 RISK ASSESSMENT

PRIVACY HARMS

According to NICR officials, a risk assessment on privacy was conducted prior to the enactment of the Act, even though the outcome was not published. To reflect this, the Act provides for the protection of privacy by restricting access to the register without authorisation by the director.[151] Section 7 is dedicated to data security.[152] Section 7 paragraphs (1) and (2) prohibit the publication or conveyance of information in the register to any person, except for the purposes provided for in the Act, and it reads:

> (1) A person shall not publish or communicate to any other person any information recorded in the register or an identity card except for –
>
> a) Purposes of this Act;
>
> b) Judicial proceedings; or
>
> c) The performance of his or her functions in terms of any other law
>
> (2) A person who comes into possession of information which to his or her knowledge has been communicated to him or her in contravention of this Act, shall not publish the information or communicate it to any other person." [153]

The purposes for which data may be shared with third parties which are outlined in the Act are:

> "...the performance or conclusion of a contract with the person to whom the information relates, for fraud prevention and fraud detection, or to uphold the legitimate interests of the requestor for verification of particulars entered in the Register."[154]

EXCLUSION HARMS

The risk assessment on exclusion harms would have considered the risks

151 National Identity Cards Act 2011, s.6(1)

152 National Identity Cards Act 2011, s.7

153 National Identity Cards Act 2011, s.7(1)(c)

154 National Identity Cards Act 2011, s.6(1)

of exclusion of groups of people from accessing services that are linked to authentication of the digital ID. The assessment would also have considered exclusion due to technical barriers such as the availability of high-speed network connectivity or electricity for online authentication.

The risk assessment concerning exclusion harms seems to have not taken place or to have not been thorough. For instance, the NICR could not cope with the influx of applicants at some of its centres, resulting in long queues and a backlog in the issuance of birth certificates and ID cards.[155] Over the years, the NICR has extended working hours at enrolment centres because of long queues, which was a barrier for some workers who could not register.[156] Furthermore, migrant workers based in South Africa were not able to obtain IDs because they could only be in Lesotho during holidays or weekends. Following complaints by the workers, the minister extended working hours and enrolment centres began to open on weekends. An outreach to provide registration services in specific locations in South Africa was undertaken for a few days during September 2016. [157]

People who have been resident in Lesotho all their lives, but do not have a birth certificate, are unable to register and obtain an ID card. The registration of births in Lesotho is below 50%.[158] Even though the registration of births is mandatory,[159] there is little adherence and no enforcement.[160] People often obtain a birth certificate when they need a passport (in the case of a minor below the age of 16) as required by the Passport and Travel Documents Act,[161] or if they need to apply for a national ID card (in the case of a person aged 16 and older) in terms of Section 14 of the National Identity Cards Act 2011 which reads:

> "(1) A person referred to in section 13, who wants to obtain an identity card, shall make an application for an identity card to the Director in the prescribed form.
>
> (2) An application made in accordance with subsection (1) shall be accompanied by the following –

155 *https://lestimes.com/registry-offices-opened-at-maseru-mall/ https://lestimes.com/registry-offices-opened-at-maseru-mall/*

156 *https://www.gov.ls/home-affairs-extends-working-hours/*

157 *https://www.youtube.com/watch?v=kDMvVQUGETg*

158 *https://data.worldbank.org/indicator/SP.REG.BRTH.ZS?locations=LS*

159 Children's Protection and Welfare Act (2011), s.8 *https://data.unicef.org/crvs/lesotho/*

160 Registration of Births and Deaths Act (1973), s.3 *http://citizenshiprightsafrica.org/wp-content/uploads/2020/05/Lesotho-Births-and-Deaths-Registration-Act-1973.pdf*

161 Lesotho Passports and Travel Documents Act 2018. s.10(2)(c)(ii). *http://citizenshiprightsafrica.org/wp-content/uploads/2020/09/Lesotho-Passports-and-Travel-Documents-Act-2018.pdf*

(a) a birth certificate or a certificate of naturalisation or registration or an indefinite residence permit;

(b) prints of all fingers of the applicant taken by an officer of the department responsible for identity cards;

(c) a photo was taken by an officer in the department responsible for identity cards; and

(d) any other requirements or documentation that the minister may prescribe."[162]

At times people have struggled to obtain a birth certificate or equivalent in order to apply for an ID card even though the requirements were reduced after the public outcry in 2014.[163] The risk assessment seems to have not taken into account the level of development of the country's birth registration regime and the circumstances of the rural population, who live in areas without roads or health infrastructure nearby. NICR registration services are in town centres, and some people have to travel long distances to register births and deaths. There are reports of people being forced to sleep on pavements while waiting to be served when offices open the next day.[164] As a result of the difficulties people face, in 2020, there were 200 000 (15%) eligible citizens who had not obtained an ID card.[89]

In conclusion, it seems that risk assessments on the exclusion harms were either not conducted or were not thorough. Otherwise the exclusion of 200 000 people, including workers and people who live in inaccessible rural areas, would have been avoided. The exclusion of refugees would have also been avoided. In 2019, the refugee population was 143.[165]

The risk assessment seems to have taken into account the risk of exclusion due to technological readiness, because the Lesotho digital ID service includes the issuing of identity cards. Users have the option of offline verification. Verification using the ID card mitigates risks due to network failures or electricity outages. Having the alternative to present an ID card is important in Lesotho because of the low electricity penetration rate and poor mobile network coverage in some areas.

162 National Identity Cards Act 2011. (Lesotho). s.14(2)(a)

163 *https://lestimes.com/molapo-eases-id-requirements/*

164 *https://citizenshiprightsafrica.org/lesotho-72-000-register-for-birth-certificate/*

165 *https://data.worldbank.org/indicator/SM.POP.REFG?locations=LS*

DISCRIMINATION HARMS

A risk assessment on discrimination harms might have been conducted because the Act is clear on the people who are eligible to be included in the Register,[94] who are eligible for an identity card. That clarity reduces the risk of discrimination that applicants might otherwise face, in particular minority groups, such as people whose mother tongue is not Sesotho or those who are from different ethnic backgrounds. However, it seems the harm of discrimination against refugees was not considered. A potential source of discrimination harm that seems to have been overlooked in drafting the Act is the fact that not all people have fingerprints. The Act does not provide for other biometrics that a person may use instead.

5.2 DIFFERENTIATED APPROACHES TO RISK

Allowing indiscriminate access to the register poses a risk of unlawful surveillance which should have been considered prior to enacting the law. The Act should have provided for a differentiation in data requests so that, for purposes of law enforcement and public order, data could be provided on the basis of a court order, and such data could be provided outside the system (e.g. by copying the concerned records to a different medium for the purpose of sharing).

The Act does not seem to have considered the risk of harm emanating from mandating the use of the national ID card as the sole method of identification and the digital ID as the single source of identity verification and authentication. Without an ID card, a person cannot obtain a driver's licence or a passport, open a bank account or register a mobile device or SIM card. The option to have other types of ID has been eliminated by a web of regulations and laws which mandate the use of the national ID card.

It appears that, in conceptualising the Act, some consideration was given to the sensitivity of permitting use. For example, Section 6 (2)(a) indicates that the director may, subject to the minister's approval, authorise the provision of information in the register "to a third party in accordance with the instruction of the person to whom the information relates". Therefore, there are cases where access would depend on the third party having to first seek consent before accessing a person's information in the register.

In order to avoid harm due to authentication errors caused by technological failures, the digital ID system allows for multiple approaches for authentication. For example, for mobile money KYC purposes, customers may use the USSD system and supply their names and national ID number. In other situations, multiple methods are to be used at the same time. An example is the Communications (Subscriber Identity Module and Mobile Device Registration) Regulations, 2021, which require both the ID card and fingerprints for authentication and verification against the register. Since the regulations came into force in May 2021, there has not been an evaluation of their implementation.

5.3 PROPORTIONALITY

This section assesses whether the envisaged governance is proportionate to the likelihood and severity of the possible risks of its use. Discussed below are the risks of inaccurate data collection, authentication errors, mission creep, indiscriminate data sharing and identity theft, and how the envisaged governance framework would ensure that the benefits are proportionate to the likelihood and severity of the possible risks.

INACCURATE DATA COLLECTION

It seems that a risk assessment for inaccurate data collection was conducted prior to passing the law. Section 2 paragraph (2)(b) reads:

> (2) The register is established to -
>
> > "...ensure the existence of accurate and reliable information about the person referred to in paragraph (a)"

and section 8 of the Act reads:

> "(1) The Director shall take reasonably practicable steps to ensure that personal information entered in the register is complete, accurate and updated where necessary.
>
> (2) The Director may require a person, Government department or statutory body that may have information or a document which could be used to verify or validate information -
>
> > (a) recorded in the register; or
> >
> > (b) provided to the Director for the purpose of being entered in the register,
>
> to provide the information or produce the document.
>
> (3) Every person to whom an identity card has been issued shall notify the Director about every -
>
> > (a) change of circumstance affecting the information recorded about him or her; or
> >
> > (b) error [*sic*] in that information of which he or she is aware."

Section 17 is further proof that the accuracy of data was a paramount consideration in the conceptualisation of the Act. Paragraph (1)(a) provides for the cancellation of an identity card if the card was issued based on inaccurate or incomplete information.

While much attention may have been given to the risk of inaccurate data

collection and the Act makes provision for managing it, the Act does not provide for oversight mechanisms to ensure that accuracy. In response to a similar risk, the Lesotho Passports and Travel Documents Act, 2018, has a specific section that deals with the accuracy of biometric data capture during the passport application process:

“Establishment of biometric system

4. (1) There is established a biometric system, in the department, which shall be maintained by the Director.

(2) The biometric system is established to -

(a) capture a biometric sample from an applicant for the machine readable passport;

(b) extract biometric data from the biometric sample;

(c) compare the specific biometric data value with that contained in one or more reference templates;

(d) decide how well specific biometric data value and the biometric sample match; and

(e) indicate whether or not an identification or verification of identity has been achieved."

It is possible that the register follows a similar process as the above because the NICR is the same issuing entity for the digital ID and the digital passport.

AUTHENTICATION ERRORS

Section 4(6) lists the identity number as one of the particulars to be included in the register about a person. By doing this, the Act provides for the use of the ID number for verification, in addition to the option of using biometric data. However, the Act does not provide for an alternative means of identification in case of authentication errors. Instead paragraphs 4(5) and4(6) provide for the owner of the information to request corrections. Until corrections are made, the owner of the information may not be able to access various services. Similarly, if an ID card is lost, the Act provides for cancellation and replacement, but it does not provide for alternative means of identification that a person may use until a new ID card has been issued or corrections have been made.

A critical source of authentication errors is the unavailability of the register for technical or administrative reasons. For example, in September 2018, newspapers in Lesotho reported that the services provided by the NICR had been suspended because the company which the government had contracted to supply and operate the platform on which the digital ID is based had stopped working

over non-payment.[166,167] Services also stopped in 2019 over non-payment of contract fees by the government.[168,169] The experience of the past years indicates that there will be times in the future when the whole system or parts of it do not work, thus affecting access to authentication services.

MISSION CREEP

As discussed earlier, the Act has mission creep built in and there are no safeguards for managing it. One safeguard that could have been considered is the requirement to have a risk management framework and annual reporting to parliament.

INDISCRIMINATE DATA SHARING

The registry is designed and optimised for data sharing. The Act gives discretionary powers regarding which actors may be given access to the data in the registry. The Act specifically provides for access by state agencies and private entities involved in the businesses of banking, insurance, credit provision and credit bureaus. The access is managed through MOUs and NDAs. There are no regulations on the security management of this ecosystem.

IDENTITY THEFT

If the digital identity of a person in the registry were to be stolen, several other identities, such as their passport, driver's licence and voting card, would be compromised because they are based on the digital ID in the registry.

5.4 RESPONSE TO RISKS

Response strategies in the law and the regulatory framework vary depending on the risk. Multiple identification options address exclusion risks while privacy by design reduces privacy-related risks.

PRIVACY HARMS

As a response to privacy harms, privacy by design is a strategy that might have been considered by the NICR; however, it is not explicitly stated in the Act. Instead, Section 7 paragraph (5) makes it an important consideration by the director because it reads:

166 *https://lestimes.com/ministry-stops-issuing-passports-ids/*

167 *https://sundayexpress.co.ls/nikuv-hits-back-at-govt-over-passports/*

168 *https://www.thereporter.co.ls/2019/09/24/passports-saga-endangers-lives/*

169 *http://publiceyenews.com/raw-nikuv-deal-haunts-lesotho-passports/*

> "The Director shall have due regard to generally acceptable information security practices and procedures which may apply to public registers of personal information."[170]

The Act makes it a crime to publish or communicate to any other person any information recorded in the register unless such publication or communication is provided for in the Act. The offence carries a fine of M 25 000, which is equivalent to ZAR 25,000 or about USD 1,800.

Privacy is also addressed in the Statement of Objects and Reasons of the National Identity Cards Act, 2011, paragraph 4, which reads:

> "In order to ensure the right to privacy of individuals as enshrined in the Constitution, the Bill provides for data privacy whereby the individual's data or information is to be treated with utmost care and confidentiality. This right to privacy, however, is curtailed in instances where verification of information is needed by Government departments for the purpose of keeping law and order, public safety, health, prosecution or judicial proceedings and also where an individual has authorised disclosure of his or her data to a third party. The third party shall, however, not pass or publish the information to another under any circumstances."

Digital ID data has linkages to financial data, because banks and mobile money have connected to the register for the purpose of verifying the identity of their customers. There is a risk of stolen identity information being used to commit fraud. However, no data on fraud incidents enabled by Lesotho digital ID data theft could be found. Nonetheless, some of the banks in Lesotho address the risk of identity theft in their customer security awareness information.[171] All banks have also introduced multi-factor authentication for online transactions to increase security and ensure notifications are sent for every transaction.[172,173]

The National Identity Cards Act 2011 and the Data Protection Act 2011, according to the World Bank Group, were passed in order to facilitate the provision of a national biometric ID as a foundation for other critical government systems.[174] The Data Protection Act was passed in February 2011, while the

170 National Identity Card Act 2011, (LSO), s.7(5)

171 *https://www.nedbank.co.ls/content/nedbank-lesotho/desktop/lt/en/business/toolsandguidance/bank-anytime-anywhere/fraud-awareness/identity-theft.htmlhttps://www.nedbank.co.ls/content/nedbank-lesotho/desktop/lt/en/business/toolsandguidance/bank-anytime-anywhere/fraud-awareness/identity-theft.html*

172 *https://www.lpb.co.ls/privacy-policy/*

173 *https://www.fnb.co.ls/security-centre/protect-yourself.html*

174 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

National Identity Cards Act 2011 was passed in March of the same year. However, the Data Protection Act 2011 was not implemented; a regulator for it has not been established to enforce the law. A functioning data protection regulator is required to ensure the protection of the privacy rights of digital ID registrants and national ID card bearers. The Data Protection Act itself needs to be updated in line with international best practice such as the GDPR.[175]

EXCLUSION HARMS

Beginning in 2014, the ministry started a mobile programme whereby officials visited villages to facilitate the issue of birth certificates.[176] To further ease the burden for rural dwellers, the ministry has started an outreach programme to travel to remote villages to facilitate the issue of ID cards. Over 6 000 cards have been issued through this outreach programme since it started.[177]

The demand from service providers to conduct biometric authentication is increasing and the NICR system needs to be improved to increase the service providers' ability to conduct biometric authentication.[178] According to the World Bank Group, the data privacy and protection functions also need to be improved. Among other things, this will ensure that as the implementation of The Communications (Subscriber Identity Module and Mobile Device Registration) Regulations, 2021 gets underway, there are no capacity constraints that may slow down the pace of registering SIM cards and mobile devices by the deadline of November 2021.

DISCRIMINATION HARMS

The NICR has addressed risks that might result in discrimination harms, e.g. by issuing ID cards for free when people register and by having the cards as an option for identification in situations where the use of biometric scanning or validation using the ID number is not possible. However, the Act does not provide alternatives for people without limbs or those who have impaired fingerprints. They are not given the option of other biometrics, such as the iris or voice, to use instead.. This can lead to people being discriminated against on account of the physical conditions of their fingers.

175 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

176 *https://sundayexpress.co.ls/government-takes-id-registration-to-the-people/*

177 *https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center*

178 *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

IDENTITY THEFT

One way to mitigate identity theft is to control access to the register by an authorised person, in addition to operational security controls. According to the World Bank Group, government systems had access to the national ID platform for making queries. A few of them, such as the Ministry of Communications Science and Technology's e-services platform, the ministries of labour tourism and public service, as well as the Old Aged Pensions agency were provided with the ability to query the register. Providing only the ability to query minimises the risk of identity theft. The risk would be increased if third parties had access to download or make copies of data from the register because this would pose a greater risk of identity theft.

In addition to operational considerations, the Act also provides some safeguards to reduce risk. Section 7, which deals with data security, provides several safeguards to minimise the risk of data theft. In relation to third parties accessing the data in the register, paragraph (6) reads:

> "A third party accessing information from the register on the authority of the Director shall treat personal information which comes to his or her knowledge as confidential and shall not disclose it unless required by law or in the course of proper performance of his or her duties."[179]

Furthermore, Section 7[180] makes the director accountable for implementing generally accepted information security practices and to maintain security measures to prevent, among other things, unlawful access to personal information entered in the register. However, these measures are not adequate, because the Act does not provide for a risk management framework and independent annual auditing of the platform and security practices; it also silent on legislative oversight. Furthermore, the Act does not provide for measures that may be taken by the information owner in the case of a detected or suspected identity theft to once again obtain a trusted digital identity. The NICR should consider issuing notifications to inform owners when their data has been accessed by third parties; this would serve as an early warning mechanism in case of identity data theft.

Paragraph 19 (b)[181] of the Act criminalises actions that can form identity theft, and it reads: "a person who, having come into possession of an identity card which belongs to another person – (i)presents it as his or hers ...." commits a crime.

179 National Identity Cards Act 2011, s.7(6)

180 National Identity Cards Act 2011, s.7(3) – (7)

181 National Identity Cards Act 2011, s.19(b)

CONCLUSION AND RECOMMENDATIONS

The digital ID in Lesotho is in a developmental phase. The implementation of digital ID passes the test of legality because the National Identity Cards Act 2011 provides for the collection of personal data, including biometric data, for purposes specified in the Act (such as the issuance of a national ID) and identity verification. The purpose of the digital ID, however, is not well articulated in the Act. The purpose is found in statements made by the director or the minister in the media or some reports. Use of the digital ID is mandatory for all people who are eligible to register. By doing this, the law introduces risks of exclusion for eligible people, who, for various reasons, may not be able to register as the Act does not provide for the use of multiple types of ID. With digital ID, identity theft is one of the most significant concerns. While the National Identity Cards Act, 2011 has provisions for the protection of data held in the register, and the Data Protection Act 2011 has provisions for the protection of personal data in general, which would be applicable to the register, there is no oversight to ensure compliance.

The concerns raised in this report can be addressed in different ways by different actors. The following recommendations are made:

It is recommended that **civil society**:

- advocate for legislation and regulatory oversights to protect privacy of personal data;
- sensitise citizens about risks inherent in personal data stored in this manner so that they may manage some of the risks.

The main recommendation to **policymakers** is to amend the National Identity Cards Act or repeal it and pass a new law to replace it. Lesotho's digital identity legislation could be improved by:

- ensuring that there is clarity of purpose;
- removing the mandate to use the ID card issued by the Act as the only means of identification. The new law should allow for other means of identification depending on the application and the risks involved;
- ensuring data minimisation. The register must contain only personal data that is required to identify a person;
- including options for biometric data that a person provides – the Act only provides for fingerprints;

- addressing privacy risks, exclusion risks and mission creep risks;
- providing for redress mechanisms to deal with registrants' and applicants' grievances without having to seek external remedies;
- introducing a separation of roles so that there is a regulator, an administrator for the register, and actors authorised to enrol those eligible for the digital ID;
- mandating transparency and accountability by requiring external annual financial and risk audits and a report to parliament;
- conducting risk assessments and human rights impact assessments to avoid the risks to personal privacy and exclusions harms that have been identified in this case study;
- fostering transparency in granting access to the register; information on which entities have been granted access should be published so that citizens know and can be on the lookout for abuses;
- ensuring the transparency of the terms and conditions, including fees payable for access by third parties; terms of access and costs should also be published in the government gazette for transparency and to avoid discrimination.

The digital ID environment in Lesotho requires robust data protection and cybersecurity policy and legal frameworks, both of which are currently lacking. The MoHA should repeal the Data Protection Act 2011 and develop a new data protection law that is more in line with modern data protection laws and conventions. To ensure implementation, the government should have a budget for the implementation of the new data protection law. Furthermore, the country should pass the current Computer Crime and Cybercrime Bill[182] which has been in draft for several years.

It is recommended that **technologists** implement digital ID solutions that are suited to the target population. The technology choices should take into account the fact that biometric online authentication and verification may be affected by the quality of connectivity in some places in Lesotho; some places do not have access to electricity and users have limited, if any, digital skills. They should also implement solutions that are secure by design.

Further research is recommended. Due to the limitation of time, it was impossible to assess the impact of digital ID governance on individuals to

182 *https://ictpolicyafrica.org/es/document/7hwpifnqr6l*

establish the extent to which the identified risks and harms affect citizens, especially women, rural dwellers, and vulnerable members of society like orphans and the aged. Future research should also look into the extent to which law enforcement agencies access data in the register, reasons for access, and impact on affected persons.

A recommendation to **donor agencies**, particularly those working the MoHA in the implementation of the digital ID, is to encourage policymakers to review the National Identity Cards Act 2011 and the Data Protection Act 2011 and introduce legislation that better protects personal data and cybersecurity.

REFERENCES

Boloetse, K. (n.d) “Raw Nikuv deal haunts Lesotho passports”. *Public Eye*. Available at: *http://publiceyenews.com/raw-nikuv-deal-haunts-lesotho-passports/* (accessed 10 June 2021).

Bureau of Statistics. (2021). 2019 Labour force survey (LFS) report. Statistical Report No.5 of 2021. Available at: *http://www.bos.gov.ls/Publications.htm* (accessed 27 April, 2021).

Central Bank of Lesotho. (2008). “Lesotho national identification card system as a prerequisite for the establishment of a credit bureau: implications for finance access and economic growth.” Available at: *https://www.centralbank.org.ls/images/Publications/Research/Reports/MonthlyEconomicReviews/2008/Economic_Review_June_2008.pdf* (accessed 29 April 2021).

Constitute. (2021). Lesotho’s Constitution 1993 (rev. 2018). Available at: *https://www.constituteproject.org/constitution/Lesotho_2018.pdf?lang=en* (accessed 31 August 2021).

Davis, B., Silvio Daidone, S. & Dewbre, J. (2015). The Impacts of the Child Grants Programme in Lesotho. International Policy Centre for Inclusive Growth. One pager No. 281. Available at: *https://ipcig.org/pub/eng/OP281_The_Impacts_of_the_Child_Grants_Programme_in_Lesotho.pdf* (accessed 9 September 2021)

Government of Lesotho. (2020). NISSA enumeration launched. Available at: *https://www.gov.ls/nissa-enumeration-launched/* (accessed 9 September 2021).

Independent Electoral Commission. (2018). Requirements in registration. Available at: *http://www.iec.org.ls/requirements-in-registration/* (accessed 31 August 2021).

Kuziński, D., Sopek, M & Trypuz, R. (N.D) A blueprint for the architecture of fully infrastructural and foundational Digital Identification systems based on the blockchained Semantic Approach. Available at: *https://lei.info/portal/wp-content/uploads/2020/04/whitepaper_lei.pdf*

Lesotho Citizenship Order 1971 [Lesotho], Order No. 16 of 1971, 1971. Available at: *https://www.refworld.org/docid/4c5849ad2.html* (accessed 12 June 2021).

Lesotho Passports and Travel Documents Act 2018.[Lesotho]. Available at: *http://citizenshiprightsafrica.org/wp-content/uploads/2020/09/Lesotho-Passports-and-Travel-Documents-Act-2018.pdf* (accessed: 28 April 2021).

Lesotho Times (2013). “IDs for all Basotho: mission impossible.” *Lesotho Times*, 19 September 2013. Available at: *https://lestimes.com/ids-for-all-basotho-mission-impossible/* (accessed 27 April 2021).

Kampong, L., Shale, T., Bhandari, L. Bhattari, P., Dahal, P., Rijal, S., Pervez, K., Khoso, M., Khan, Q. & Denisova, A. (n.d.) Alternative Payment Systems: Experiences from Lesotho, Nepal and Pakistan. Available at: *https://olc.worldbank.org/sites/default/files/6.%20Alternative%20Payment%20Systems%20-%20Experiences%20from%20Lesotho,%20Nepal%20and%20Pakistan%20_0.pdf* (access 9 September 2021).

Money Laundering and Proceeds of Crime Act 2008 [Lesotho]. Available at: *https://fiu.org.ls/legislation/Money_laundering_&_Proceeds_of_Crime_Act.pdf* (accessed: 28 April 2021).

National Identity Cards Act 2011 [Lesotho].

Ntaote, B. (2014) "Nikuv Hits Back At Govt Over Passports". Sunday Express, 21 September 2014. Available at: *https://sundayexpress.co.ls/nikuv-hits-back-at-govt-over-passports/* (accessed 31 August 2019).

Ntaote, B. (2013). "Molapo-eases-id-requirements" Lesotho Times, 31 October 2013. Available at *https://lestimes.com/molapo-eases-id-requirements/* (accessed 31 August 2021)

Ort, R & Raboletse, T. (2021 February). National ID in Lesotho is putting citizens at the center. World Bank Blogs: Governance for Development. Available at: *https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center* (accessed 9 June 2021)

Petlane, T. (2013) "African Integration: What do New National IDs in Lesotho and South Africa Mean?". South African Institute of International Affairs (SAIIA), Available at: *https://saiia.org.za/research/african-integration-what-do-new-national-ids-in-lesotho-and-south-africa-mean/* (accessed 31 August 2021).

Pivcevic, K. (2021). Lesotho national digital identity system within 200,000 of universal coverage, saving public money. Available at: *https://www.biometricupdate.com/202103/lesotho-national-digital-identity-system-within-200000-of-universal-coverage-saving-public-money* (accessed 22 April 2021).

Public Finance Management Act (LSO) Available at: *http://www.finance.gov.ls/documents/laws%20and%20regulations/PFMA%20Act%202011.pdf* (accessed 10 June 2021).

Raboletsi, T. (2016). How to successfully implement ID cards and national registration: the Lesotho perspective. Available at: *https://id4africa.com/2015/presentations/31_Tumelo_Raboletsi.pdf* (accessed 11 June 2021).

Raboletsi, T. (2019). The Multiplier Effect of Digital ID and Financial Inclusion in Lesotho. Available at: *https://www.id4africa.com/2019_event/presentations/InF6/2-Tumelo-Raboletsi-Lesotho.pdf* (accessed 31 August, 2021).

SABC News. (2016,). "The Lesotho birth certificates campaign still underway". Available: *https://www.youtube.com/watch?v=kDMvVQUGETg* (accessed 31 August 2021).

Sello, L. (2016). "Registry offices opened at Maseru Mall". *Lesotho Times*. 20 May 2016. Available at: *https://lestimes.com/registry-offices-opened-at-maseru-mall/* (accessed 31 August 2021).

The Parliament of Lesotho. (2011). *Statement of Objects and Reasons of the National Identity Cards Act, 2011*. Government Notice No. 21 OF 2011.

The Parliament of Lesotho. (2018). "Statement of Objects and Reasons of the Lesotho Passports and Travel Documents Act, 2018." Government Notice No. 15 OF 2018. Available at: *http://citizenshiprightsafrica.org/wp-content/uploads/2020/09/Lesotho-Passports-and-Travel-Documents-Act-2018.pdf* (accessed 10 June 2021).

The Refugee Act 1983 [Lesotho]. Available at: *https://www.refworld.org/docid/3ae6b4f024.html* (accessed 30 April 2021).

The Reporter. (2019) "*Passports saga endangers lives*". The Reporter 24 September 2019. Available from: *https://www.thereporter.co.ls/2019/09/24/passports-saga-endangers-lives/* (accessed on 12 June 2021).

UNCTAD. (2021). "UN list of least developed countries." Available: *https://unctad.org/topic/least-developed-countries/list* (accessed 30 April 2021).

UNCTAD. (n.d). "The unctad b2c e-commerce index 2020." Available: *https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf* (accessed 31 August 2021).

UNCTAD.(n.d) Spotlight on Latin America and the Caribbean. Available at: *https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf* (accessed 10 June 2021).

UNHCR (2021). States parties, including reservations and declarations, to the 1951 Refugee Convention. (September 2019). Available at: *https://www.unhcr.org/5d9ed32b4* (accessed 30 April 2021).

UNHCR (2021). States parties, including reservations and declarations, to the 1967 Protocol Relating to the Status of Refugees. Available at: *https://www.unhcr.org/5d9ed66a4* (accessed 30 April 2021).

UNHCR. (2019). Submission by the United Nations High Commissioner for Refugees for the Office of the High Commissioner for Human Rights' Compilation Report - Universal Periodic Review: 3rd Cycle, 35th Session Kingdom of Lesotho. *https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=7626&file=EnglishTranslation* (accessed 10 June 2021).

United Nations Conference on Trade And Development (UNCTAD). (2019). Lesotho rapid eTrade readiness assessment. Available at: *https://unctad.org/system/files/official-document/dtlstict2019d8_en.pdf* (accessed 10 June 10, 2021).

United Nations.(2021). "E-Government Development Index". Available at: *https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/95-Lesotho/dataYear/2012* (accessed 31 August 2021).

Vrinda Bhandari, S. (2020) “Governing ID: Introducing our Evaluation Framework.” Digital Identity Design and Uses. Available at: *https://digitalid.design/evaluation-framework-02.html* (accessed 26 April, 2021).

World Bank Group. (2014) “Digital Identity Toolkit: a guide for stakeholders in Africa.” Available at: *https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf?sequence=1&isAllowed=y* (accessed 31 August 2021).

World Bank Group. (2020). “Lesotho digital economy diagnostic.” Available at: *https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y* (accessed 27 April 2021).

World Bank Group. (2021). “Lesotho social protection programs and systems review.” Available at *https://documents1.worldbank.org/curated/en/996831624982907050/pdf/Lesotho-Social-Protection-Programs-and-Systems-Review.pdf* (accessed 9 September 2021).

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. ■