Digital Identity in South Africa

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

RESEARCH & WRITING
Gabriella Razzano

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 South Africa

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 South Africa

By Gabriella Razzano, Research ICT Africa

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, Tanzania, Uganda, and Zimbabwe.

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.

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 South Africa case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Gabriella Razzano, Research ICT Africa. 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 Gabriella Razzano 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

The South African project to digitise its foundational identity expands on a broad system of paper identity documents underpinned by an identity database that has for many decades included records of biometric identity, primarily through fingerprints. It is being driven through a phased introduction of Smart ID Cards.

The empowering statute, the Identification Act, is from 1997, and long preceded the introduction of broad-based personal data and privacy protection found in the 2013 Protection of Personal Information Act. This provides a patchy basis for protections, especially in the absence of any guiding policy framework, which makes the mitigation of risks challenging.

The recent draft Official Identity Management Policy (2020) indicates a desire to modernise government identity management and align with national development objectives. There are strong indications though that such policies may be insufficient to manage the realities of personal data risks that accompany digitisation efforts, without the full and purposeful implementation of the Protection of Personal Information Act across stakeholder groups. This is concerning, given the imperatives for universal digital identification, in light of the lived experience of poor service delivery in the realm of identity management for South African citizens and non-citizens alike.

ACRONYMS AND ABBREVIATIONS

ABIS	Automated Biometric Identification System
DHA	Department of Home Affairs
HANIS	Home Affairs National Identity System
ID Act	Identification Act, 1997`
IRSA	Information Regulator of South Africa
NIS	National Identity System
NPR	National Population Register
PAIA	Promotion of Access to Information Act, 2002
POPIA	Protection of Personal Information Act, 2013

CONTENTS

INTRODUCTION

National identity in South Africa is represented through a green bar-coded paper document, although a phased roll-out process has started to replace all such documents with a Smart Identity Card (Smart ID) (Government of South Africa, n.d.). The Smart ID card has on its face a person's name, identity number, citizenship status, sex and country of birth. The Smart ID card also securely stores biometric information (face and fingerprint currently) used for authentication, and has space to store additional secure information like voter information. South Africans are currently not obliged to hold a Smart ID Card, but all newly issued identity documents are in the form of the Smart ID. However, Smart ID cards can only be issued from offices that have the "live capture system", which is the system used to process individuals into the system (Western Cape Government, 2021). Additionally, they can be obtained through certain banks that use the system in-house (providing a very literal example of the associations between digital identity and financial services) (MyBroadband, 2020).

1.1 CONTEXT

This functional digital identity system is largely empowered through a statute from 1997 called the Identification Act (ID Act), which has been attenuated by the more recent data protection law, the Protection of Personal Information Act, 2013 (POPIA). The ID Act provides the foundations for the statutory empowerment of identity, while the POPIA prescribes the grounds for lawful processing of personal information from private and public sector actors.

While there is broad coverage of national identity among South African citizens, the United Nations still estimates that 137 million people in Southern Africa are essentially "stateless" through lacking the necessary identity documentation (UNHCR, 2020). An estimated 15 million of them - of which roughly 3 million are under the age of 18 - reside in South Africa (Lawyers for Human Rights, 2021). As an additional consideration for the lived experience of identity, the Department of Home Affairs (DHA) in South Africa has historically been marred by incredible challenges in service delivery, resulting in long queues for citizens and administration inefficiencies.

South Africa suffers from significant social and income inequality, with its Gini coefficient measured at a startling 0.63 in 2015. A consequence of this inequality is the need for a significant social protection network. Statistics South Africa released the results of its General Household Survey in 2018, indicating that 45.2% of households interviewed depend on social grants, which renders over 17 million people reliant on these grants from the state (Statistics South Africa,

2018). Social grants are currently distributed by the South African Social Security Agency (SASSA) into accounts provided by the personal banking arm of the South African Post Office (SAPO). Digitalised identity is central to accessing these benefits.

South Africa's inequality also has digital dimensions, though it has comparatively high Internet penetration in contrast to many countries in the region, at over 50% Internet penetration and 84% mobile phone penetration (although with only 11% household penetration) (Gillwald & Mothobi, 2019).There are also significant dimensions of inequality in access across gender, location and education lines (Gillwald & Mothobi, 2019).

1.2 HISTORY

South Africa's identity system has long been predicated on expansive incorporation of biometrics (Breckenridge, 2014), but also struggles as a result of significant decentralisation of collection and storage.

Yet grand "panopticon" style centralisation of national identity ambitions like the DHA's Home Affairs National Identity System (HANIS)[9] emerged outside of an existing data governance protection framework, and the National Population Register (NPR) was enabled to store biometric data as far back as 1982 (Breckenridge, 2005).

A revision of the system has been articulated in the 2020 Draft Official Identity Management Policy, hereinafter referred to as "'the Draft Policy"', which was recently released as part of a public consultation process. A motivation for this revision is the need for sound digital identity management to facilitate trade, business and digital economy components of the Fourth Industrial Revolution (DHA, 2020b). Yet these ambitions for digital efficiencies exist within a reality of logistical failings through its own existing digital infrastructure. As the Portfolio Committee on Home Affairs itself noted "...the glaring and perpetual long queues that are evident at service points indicate the far-reaching implications of the impact of the lack of improvement within the IT environment" (BusinessTech, 2021).

1.3 METHODOLOGY

Given the intended focus of the tool, the South African case study focuses on the South African national identity project, under which identity is managed through the National Population Register (NPR). The NPR manages biographical information in compliance with the ID Act, and is overseen by the DHA. It is

9 See further the Criteria for Case Selection explanations on HANIS, etc.

specifically limited to citizens and permanent residents. Iit is envisioned this will be replaced by a centralised National Identity System (NIS) (DHA, 2020). This tracks with the concept of a "foundational identity system" (Bhandari *et al.*, 2020).

Additionally, the HANIS is used to store and process the biometric data of citizens and non-citizens (refugees, asylum seekers, illegal foreign nationals and permanent residents). This system will reportedly be replaced in the near future by the Automated Biometric Identification System (ABIS), which will process and store biometric data of all persons, citizens and noncitizens (DHA, 2020).

1.4 RESEARCH DESIGN

The research design was constrained by the utilisation of the "Governing ID: A Framework for Evaluation of Digital Identity — The Centre for Internet and Society" (Bhandari *et al.*, 2020).

1.5 DATA COLLECTION

A variety of data collection activities was incorporated, with secondary data chiefly sourced through an extensive literature review (see the Reference List outlined in detail below). Interviews were conducted with different interviewees, but these largely only informed analysis as secondary sources, rather than serving as primary data. However, data from one interview was influential (see below).

In terms of primary data collection, the following data sources were reviewed:

- Extensive review of parliamentary records (equivalent to Hansard records) made openly available through collaboration with the National Parliament on the Parliamentary Monitoring Group (https://pmg.org.za/);
- The review of draft policy opened as part of public participation processes, namely the "Draft Official Identity Management Policy, 2020" from the DHA and the "Draft Data and Cloud Policy, 2021" from the Department of Communications and Digital Technologies; and
- Expert interview - on 30 April 2021, an interview was conducted with a civil society product owner working in a company that works on functional digital identity within the health sector. The interviewee requested to remain anonymous.

1.6 EVOLUTION OF SYSTEM

As covered in introductory sections, South Africa's national identity project is underscored by the NPR (see below an outline of the data and system for the

creation of the NPR). The roll-out of the Smart ID, which is the digitalised version of the South African document-based system, is underway.

The national identity project in South Africa comes with complications, many of which have been articulated as part of the DHA's recent Draft Policy (which stands as the most relevant and current policy intervention in the area of identity). Though national identity is the remit of the DHA, decentralisation occurs in relation to identity confirmation (DHA, 2020a). Much of this has arisen from the need to centralise a variety of different identity sources as part of South Africa's national identity project after independence from Britain and after the fall of Apartheid: this project had to try and incorporate divergent administration systems of identity that resulted from segregationist policies, alongside both colonial and Apartheid preoccupations with biometric regimes for biometric control (Breckenridge, 2005).

Transitions to new systems have also been marred by procurement challenges and controversy, as seen with the derailment of the ABIS system introduction, where the original tender was declared irregular due to "brazen" corruption in the awarding of said tender (Parliamentary Committee of Home Affairs, 2020).

As a response to challenges in national identity management, the DHA is seeking to establish a National Identity System (NIS) to replace the National Population Register (NPR). The proposed purpose of this exercise is improving national identity management for social benefit, but this new regime will emerge within a paradigm that now directly acknowledges lawful data processing in terms of POPIA (DHA, 2020b).

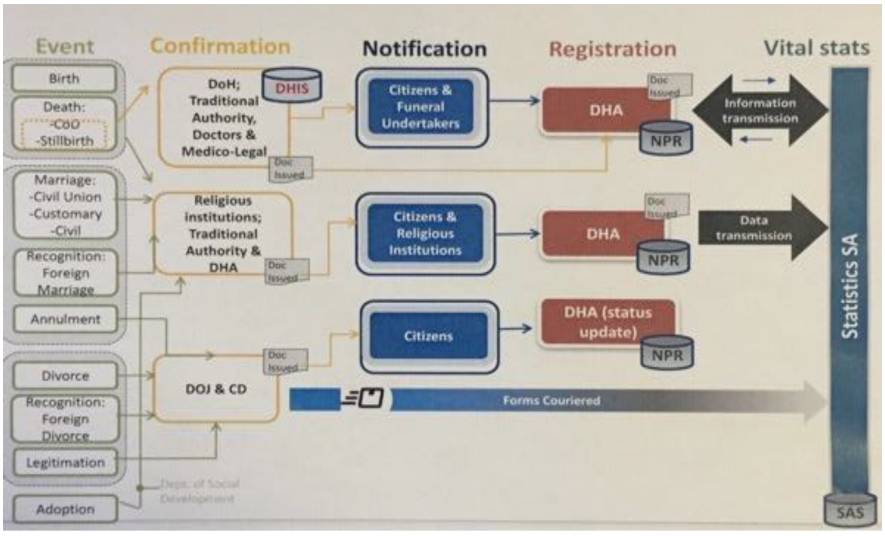


Diagram 1: An overview of the data sources for the National Population Registration (DHA, 2020b).

RULE OF LAW TESTS

2.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

The main empowering statute for the national identity programmes of the state is the Identification Act, 1997 (read with the Alteration of Sex Description and Sex Status Act 49, 2003) (ID Act). The law provides for the establishment of a NPR as the definitive source of identity, administered by the DHA:

> *"The DHA's sole mandate includes the sole authority to affirm and regulate official identity and South African citizenship" (DHA, 2020).*

The law does not exist in a statutory vacuum, and important limitations on how biometric and personal identity may be processed as part of any public activities is provided for in the Protection of Personal Information Act, 2013 (POPIA). Although the Act was fully in effect by 1 July 2020, entities were given a 12-month grace period in which to comply with its obligations. The POPIA thus only came into full effect at the time of writing (1 July 2021).

The empowering ID Act provides clear authority to the DHA to collect biographical and biometric data necessary to complete the NPR, with Section 8 explicitly providing for the collection of the following types of data:

- identity number;
- surname, full forenames, sex, date of birth and the place or country where born;
- if registrant has attained the age of 16 years, ordinary place of residence and postal address;
- if registrant is a South African citizen but is not a citizen by birth or descent, the date of their naturalisation or registration as such a citizen, and, if the registrant is an alien and was not born in the Republic, the date of their entry into the Republic, and the country of which they are a citizen;
- the registrant's fingerprints, if they have attained the age of 16 years; and
- any other particulars determined by the Minister by notice in the Government Gazette as particulars which, subject to the conditions, exceptions or exemptions (if any) mentioned in the notice, shall be included in the register.

The law clearly empowers the DHA to collate and maintain the definitive NPR.

LEGALITY

As an extension of the existing identification process, the legality of the biometric collection process as part of these activities has both been clearly mandated by the ID Act, but has also not been subject to much challenge. The Minister is empowered through the law to expand data collection sources for inclusion (see again Section 8 above), but such notices would need to be published in the Government Gazette. Regulations to the ID Act have been published under GNR.978 of 31 July 1998.

In terms of any justifiability for rights infringements, the South African Constitution in Section 36 prescribes the criteria for a justifiable limitation of rights as being:

> *"36. (1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including—*
>
> *(a) the nature of the right;*
>
> *(b) the importance of the purpose of the limitation;*
>
> *(c) the nature and extent of the limitation;*
>
> *(d) the relation between the limitation and its purpose; and*
>
> *(e) less restrictive means to achieve the purpose".*

However, there has not been any significant or specific constitutional challenges to the ID Act in relation to biometric identity processes. While the POPIA (which seeks to give effect to Section 14 of the Constitution, and the right to personal privacy that it encapsulates) will provide its own form of statutory limitation on the powers to process personal information, inclusive of biometric information, the informational dimensions of privacy rights are relatively new within the constitutional interpretative practice. This is discussed further under rights.

QUALITY OF LAW

If the quality of law is chiefly understood as an element that allows for foreseeability, the standards of publication (and public participation) which underscore democratic law-making practice are certainly assistive.

Public participation, and transparency in relation to drafting, is facilitated through the parliamentary process with Parliament holding legislative

authority (outlined by the constitutional provisions contained in Chapter 4). The transparency of the parliamentary process is greatly enhanced by the work of the Parliamentary Monitoring Group – a non-governmental organisation that not only minutes and publishes parliamentary activity, but provides this alongside tools which assist in specific Bill monitoring.[10]

The publication of laws is prescribed for through the Government Gazette, although digitisation and accessibility of the Gazettes has long been a challenge. While uniform access to digitised Gazettes is largely facilitated by private legal service providers like LexisNexis and Jutastat, non-governmental organisations have greatly and directly enhanced access to legal information. The platform Laws.Africa, which digitises African legal information for public use, is digitising and making public South African Gazettes,[11] while the Southern African Legal Information Institute (SAFLII) provides free and open access to both statute, case law and other relevant legal materials.[12]

South Africa's ID Act is therefore implemented in a context of significant statutory and parliamentary transparency, although it must be noted that functions are significantly supported by non-governmental organisations. While the DHA does not have any prescribed awareness-raising mandates in terms of the ID Act specifically, it is broadly mandated through its public administration obligations to ensure participation through sufficient provision of information on its functions.

This is interesting when compared to the POPIA which – as law designed for the regulatory context which establishes an office of the Information Regulator of South Africa (IRSA) – expressly mandates the IRSA with active awareness-training mandates in terms of the POPIA and the Promotion of Access to Information Act (PAIA). Over time, it will be interesting to observe what these differing levels of awareness-raising mandates mean for the public narratives on intersections of privacy and identity.

CLARITY AND PRECISION

Given its status as a foundational identity programme, the identity contained on the NPR is intended to be an individual's definitive citizen identification and contains biometric components for authentication. However, the passage of the ID Act well precedes the passage of the POPIA, meaning that the ID Act does not present sufficient particularity in relation to data processing standards

10 Their work can be viewed at their website here: *https://pmg.org.za/*

11 Their work can be viewed at their website here: *https://laws.africa/*

12 Their work can be viewed at their website here: *http://www.saflii.org/*

(though the POPIA is the definitive law on processing and private and public sector actors are now lawfully obliged to comply with its provisions). The DHA itself notes within its Draft Policy (which was recently released as part of a public consultation process) that there are aspects of the law that may need to be adjusted for helping to ensure better consistency" (DHA, 2020):

> *"The Identification Act and Alteration of Sex Description and Sex Status Act 49 of 2003, are key legislation that regulate how personal data that is hosted in the DHA identity management systems is handled. The legislation needs to be amended to regulate handling personal information in line with the Constitution and the POPI Act. The current practice of dumping the department's data on other government systems is contrary to the POPI requirements."*

Within the Draft Policy, there are clear attempts to align the policy with what is commonly considered as 'good' ID principles, including establishing consent as the foundation for identity governance, but this alignment is not yet reflected in statute (DHA, 2020).

2.2 LEGITIMATE AIM

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

The preamble of the ID Act defines it as needed to:

> *"To provide for the compilation and maintenance of a population register in respect of the population of the Republic; for the issue of identity cards and certain certificates to persons whose particulars are included in the population register; and for matters connected therewith".*

However, preambles are not incredibly indicative of the full range of political imperatives underscoring a digital identity project. Indications of the aims of digital identity in the context of South African development are provided for within the DHA's revision of the digital identity management policy environment.

A motivation for the revision of the national identity system is stated as the need for sound digital identity management to facilitate trade, business and digital economy components of the Fourth Industrial Revolution (DHA, 2020). Yet these ambitions for digital efficiencies exist within a reality of logistical failings through the DHA's own existing digital infrastructure. As the Portfolio Committee on Home Affairs itself has noted:

> *"...the glaring and perpetual long queues that are evident at service points indicate the far-reaching implications of the impact of the lack of improvement within the IT environment" (BusinessTech, 2021).*

Comparatively, the aim of the POPIA is unsurprisingly more protectionist than phrased in a context of innovation and/or economic imperatives, with its preamble stating:

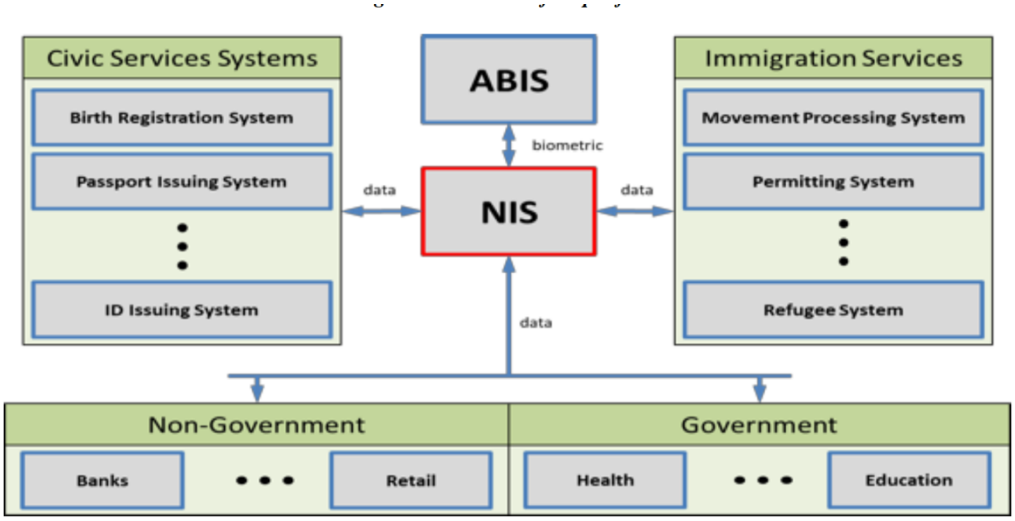
> *"To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith".*

2.3 DEFINING ACTORS AND PURPOSE

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

There is a strong focus in the Draft Policy on interoperability, and while there may of course be associations between this and broad actor use, the Draft Policy itself notes the challenges in the decentralisation of identity with the public sector itself (DHA, 2020). The complete outsourcing of technology development to external service providers in the public sector identity environment has previously resulted in "vendor lock-in" (Breckenridge, 2019). Interoperability is identified as a mechanism for overcoming this very real regional challenge. This has also resulted in tender and procurement challenges, which have directly derailed the national identity project in the past at several points, including the contract disputes that arose in the development of the HANIS system (Breckenridge, 2008).

However, while in practice the implementation of procurement public-private partnerships have presented challenges, the actors envisioned in the *use* of the digital identity system are foreseeably imagined as very broad, given its foundational identity status. The DHA offers the following as the visual frame (DHA, 2020):



In justifying this, the DHA states (DHA, 2020):

> *"All access to digital data and records will be rule-based and governed by appropriate legislation. Rules that ensure security and the rights of citizens and residents will derive from cyber security and privacy legislation. The new population register will be comprised of legally mandated records that are accurate, highly secure and linked to biometric data that relates to a unique individual. It will be the basis of a trusted official e-identity that will be the backbone of the digital platforms, State and private, that all our lives will depend on."*

The Policy expressly states its "major customers" to be "...the Department of Health, the South African Police Service, the Department of Social Development, etc." (DHA, 2020).

The exact parameters of the involvement of private actors in both design, development and utilisation of the revised NIS is thus not clear, given the status of the Draft Policy. The POPIA should ensure that no amendment to the ID Act or other legislation will create any lesser standards for data protection, regardless of the actor involved. As a fully interoperable system will broaden the possibilities for abuse significantly, it will be important to ensure that mandates are clearly articulated within enabling law and/or policy.

The existing Smart ID is a form of digital national identity (see for further reference on the original roll-out plan for the cards Appendix A), yet the current interoperability challenges practically impede an over-breadth in multi-stakeholder accessibility to the current system.

In addition, the ID Act prescribes direct limitations on access to the NPR - as the data source for the national identity system - through Section 6 (prohibiting unauthorised access) and 21 (prescribing secrecy of content on the NPR). However, the access and secrecy provisions permit the Director-General to allow

access. There is an important caveat on that access provided for in Section 21(3), which states:

> *"No information may be furnished to any organisation, body, society or institution contemplated in subsection (2)* unless the information is required for the exercise or protection of any rights, is in the public interest, or is for the compilation of a voters' roll".

However, as there is no publication requirement to the exercise of this power, the Director-General has broad powers to give direct access to the underlying NPR data that supports the NIS.

PURPOSES

Alongside the explorations of the "legitimate aim", it is worth noting that, historically, identity has generally incorporated biometric markers for identification. Yet, as the Draft Policy states, the main policy ambitions for revising the systems are to:

- enable an inclusive digital population register that is secure, accurate and confidential;
- position the DHA as the sole provider of official documentation relating to the identity of civic and international migration status of citizens and foreign nationals within South Africa's territorial jurisdiction;
- position the DHA as the sole provider of official identity and civic status verification services;
- establish rules that govern accessing and processing population register records and data in line with relevant policies and legislation, such as the POPIA and the Cybercrimes Bill;
- establish the NIS to generate critical data needed for e-government and ecommerce to function; and
- enable an application for DHA services via multiple channels (DHA, 2020).

It is seeking to do this in a context of significant fragmentation and decentralisation, and it envisions digital identity as central to accuracy and interoperability across services.

2.4 REDRESSAL MECHANISMS

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

There are no user notification provisions in relation to the existing South African digital identity systems as it relates to Smart IDs that arise from the ID Act for when your identification is used (or accessed) by another party, or from the regulatory surrounds. This should be borne in mind alongside the quite broad array of actors' permissions outlined above. However, it should also be read alongside the Draft Policy's statement of intention to centre notification under the Draft Policy's sixth principle, which covers "Protecting user privacy and control through system design" (DHA, 2020).

The POPIA has, however, altered the environment in terms of personal information specifically (whilst also providing specific access and correction rights). It creates positive obligations on both public and private bodies to notify data subjects of any breaches that have occurred in relation to their personal data (as per Section 22), and also importantly provides (in Section 18) for notification of collection of information. However, it is worth noting that the POPIA contains a general exemption against the obligation to notify of collection in terms of Section 38 if the personal data in question is being processed for the discharge of a public function – though only *to the extent* to which the application of the notification provision would be likely prejudice the proper discharge of that function.

While it is clear the POPIA legislation will likely fill important gaps in relation to data subject rights, there is still a level of obfuscation at the particular area of *use* of identity. When considering the broad range of actors the NIS is currently seeking to empower, this will be an important area to monitor, with data subject rights of access arguably not being sufficient to ensure full transparency.

ACCESS AND CORRECTION

Again, the breadth of constitutional and statutory rights and obligations provided for in the South African environment need to be reflected on to understand the specifics of the digital identity context. A broad array of specific access rights are provided for.

The ID Act provides for processes of correction, cancellation and replacement of identification documentation through the DHA through Section 19.

Access to information is chiefly given effect through the Promotion of Access to Information Act, 2000 (PAIA), which provides individuals with rights to access personal (and other) information on application to public and relevant private bodies. The PAIA also allows for other sectoral laws which may provide access to information. Of particular interest is the National Credit Act, 2005, which in

Section 72 gives individuals the right to access their credit information for free from credit bureaus, etc. Examples of other sectoral forms of access can be found, for instance, in the National Environmental Management Act, 1998 (though those are in relation to information rather than *personal* information).

The PAIA, however, preceded the POPIA, and the POPIA has provided additional and more specific data subject rights of access. Section 23 provides data subjects (once they have established their identity) with the right to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and the right to request from a responsible party the record or a description of the personal information about the data subject held by the responsible party. Additionally, there are rights to correction and even deletion contained in Section 25.

It is worth noting that these correction rights are not equivalent to a "right to be forgotten", as seen in European jurisdictions, and do not apply, for instance, to rights to de-indexing. Rather, they form a component of the rights necessary to help ensure an *accurate* and permitted digital identity for data subjects.

DUE PROCESS

As noted, the broader statutory environment helps support the rights available to data subjects and citizens more broadly. The "suitability" of these processes is difficult to assess, given they relate to a variety of contexts and conditions. Broader administrative justice rights are an important due process mechanism for public sector driven administrative actions and are chiefly given effect through the Promotion of Administrative Justice Act, 2000 (PAJA).

The PAJA states that *any* administrative action which materially and adversely affects the rights or legitimate expectations of any person must be procedurally fair. It provides for the right to receive written reasons for a decision and creates the opportunity for the judicial review of administrative action. While the remit of the law seems limited to the public sector, constitutional jurisprudence has consistently sought to create broad definitions for what is defined as "administrative action" and what constitutes an "organ of state" in seeking to extend protections for what were traditionally seen as state obligations, but are increasingly being performed by private actors (Finn, 2013; Razzano, 2020).

Certain areas within the digital identity environment may seem outside the bounds of administrative law, however. Examples are using civil redress mechanisms to deal with issues of omission or deactivation of digital ID (due to provision of false information or non-use), errors in the enrolment and verification process, or when there is an authentication failure (to prevent exclusion). However, the broad definitions of administrative action, and the application of the law to *any person*, arguably provides significant potential as a

form of recourse for data subjects moving forward.

The POPIA also creates the Office of the IRSA to provide redress for failures to comply with data protection more directly. The IRSA essentially acts as an ombudsman (with broad powers of warrant, seizure and directives, etc.) that advances the realities for access to justice, given the significant costs and delays associated with judicial review through courts. Members of the public have the right to approach the Office of the IRSA directly with complaints.

2.5 ACCOUNTABILITY

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

The fact that the POPIA imposes obligations on both public and private bodies for the lawful processing of data significantly enhances accountability within the existing digital identity environment. Accountability is enhanced by both making a mechanism available for redress and oversight in the Office of the IRSA, but also by directly establishing accountability as one of the eight lawful processing grounds, stating succinctly in Section 8:

> *"The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself".*

This subject-centred accountability framework in relation to personal data has been an important contribution of the law. In terms of the ID Act, the Director-General is in charge of the compilation and maintenance of the NPR, but this exists in a context of decentralised data management and weak cloud policy.

These kinds of challenges might be why the Department of Communications and Digital Technologies recently published a contentious *Draft National Data and Cloud Policy, 2021*, which seeks to create the policy conditions for centralised, state-owned, data management facilities for storing, and providing real-time access to, public sector data. Those will be conditions which facilitate accountability, but it seems clear that administrative law and the POPIA seek to entrench public sector accountability for digital identity management broadly.

2.6 MISSION CREEP

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

The risk of mission creep (which refers to the gradual or incremental expansion of an intervention, project or mission, beyond its original scope) is not considered within the ID Act, although the centering of the principles of "minimality" as a foundational ground for lawful data processing in the POPIA can help prevent this practice. Minimality, contained in Section 10 of the POPIA, requires: "...personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive".

The NPR has already been substantially constituted but, given that "processing" of data under the POPIA includes accessing that data (as well storing, altering or using data), the provision will be central to the future of digital identity practice. Limitations on the further processing of personal data outside their original purpose specification do also provide additional important salves to the risk of mission creep (see Section 15).

RIGHTS-BASED TESTS

3.1 NECESSITY AND PROPORTIONALITY

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

Privacy as a right[13]

South Africa's Constitution protects the right to privacy in Section 14, namely that *"Everyone has the right to privacy, which includes the right not to have…the privacy of their communications infringed".*

The direct reference to communications privacy in Section 14 has been expanded to include informational protection through case law and statute. Compared to other regional or national Constitutions, it also encompasses a relatively direct constitutional reference to information privacy (privacy is often merely captured as a form of property right in other contexts) (Razzano, *et al*. 2020). South Africa's constitutional regime is based on "no fault": once a breach is established, there is not a requirement to demonstrate fault (McQuoid-Mason, 2014). The essential structure of the constitutional provision is to outline the methods by which privacy might be infringed, i.e. through search, seizure, or communications interference, rather than to centre on what is the remit of "private" (this remit has emerged through case law).

While privacy jurisprudence in South Africa began emerging in the 1950s (Burchell, 2009), central constitutional principles began to impact its conceptualisation as the constitutional jurisprudence arose post-independence in 1994. In *Bernstein and Others v Bester NO and Others* [1996] ZACC 2, the notion of privacy began to be understood along a continuum, with Ackermann J noting:

> *"A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no*

13 Much of the proceeding work on South African privacy in the constitutional order is part of research that was undertaken by the author in partnership with the Association of Progressive Communications, which has as yet to be published.

> *justifiable limitation thereof can take place. But this most intimate core is narrowly construed."*

The right to privacy was also later explained by the Constitutional Court (CC) as the "right of a person to live his or her life as he or she pleases" (see *NM and Others v Smith and Others* (Freedom of Expression Institute as Amicus Curiae) 2007 (7) BCLR 751 (CC) at para 33), which bears similarities to the classic Warren and Brandeis definition of the "right to be let alone" (Warren & Brandeis, 1890).

Specific ideas on *informational* privacy were furthermore considered in cases like *Mistry v Interim National Medical and Dental Council and Others* [1998] ZACC 10. The CC here acknowledged that the constitutional right to privacy does not directly reference informational privacy (it refers instead to communications) but assumed it to be included in this matter. Later readings related to the right began to centre information more directly, with Judge Neethling defining privacy in 2005 as:

> *"...an individual condition of life characterised by seclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has himself determined to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private" [Emphasis added] (Naude & Papadopoulos, 2016).*

By the time the POPIA was promulgated, data rights as a form of privacy had been substantially aligned in normal discourse. The POPIA has (per its preamble) been enacted to:

> *"regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the* **right to privacy subject to justifiable limitations** *that are aimed at protecting other rights and important interests" [Emphasis added].*

The POPIA has also provided far more emphasis on personal data and individual control over one's personal data (through the specification of particular data subject rights) than its originating constitutional underpinning.

NECESSARY AND PROPORTIONATE

As addressed earlier, South African constitutional jurisprudence provides for determining the justifiability of limiting rights, which include necessity and proportionality within their tests. While no privacy challenges have been brought against the ID Act, forms of administrative challenges on components of the Act have been brought. An example is *Sibiya v Director-General: Home Affairs and Others* [2009] ZAKZPHC 6.

Besides constitutional or other jurisprudence, we can also consider the realities of the digital identity environmentto address necessity *as a broad standard*.

A particular challenge in the South African landscape has been the amount of personally identifying information included with the actual *identity number itself*, which as per the Regulations is compiled to include particulars of a person's date of birth and sex, as well as their status as a South African citizen. The identity number consists of 13 digits, which are compiled as follows:

11 1	22 2	3 3	4 4	5 5	6 6	7 7	8 8	9 9	10 10	11 11	12 12	13 13

- the first six digits represent the date of birth of the person;
- digit 7 indicates the sex of the person (being either male or female;
- digits 8 to 10, represent a serial number;
- digit 11 represents the citizenship of the person;
- digit 12 represents the index number 8, under which the person's particulars have been included in the population register; and
- digit 13 is a control figure determined by the computer.

This makes even the protection of the identity number *itself* an almost disproportionate impediment to privacy in practice. As a result, the DHA has posited replacing the identity number with a unique, random identifier instead (DHA, 2020). This additionally would go to serving to deal with the exclusions of non-binary persons currently facilitated by the identification number (Nortier, 2021).

Full compliance with the POPIA – including for instance limits on retention and use specification – go some way to creating an environment that can support the necessary and proportionate realisation of digital identity in practice, but the question necessarily then becomes if the public sector – as charged with the oversight of digital identity – is realistically capacitated to meet its compliance requirements.

3.2 DATA MINIMISATION

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

As seen, data minimisation is a central principle of the POPIA regime. Yet, as mentioned, the ID Act empowers the DHA to collect a broad array of data for the

NPR due to the civic functions that a foundational identity should fulfil.

Under the POPIA, limitations on data do not form a part of a minimisation enquiry, but rather is part of the condition relating to "purpose specification". Section 14 states (with some internal limitations expressed in more detail after) that

> *"...records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed".*

While these processing conditions contribute to a sound implementing environment for digital identity, given the early stages of the POPIA, effectiveness adjudication is still required that might shed light on how the IRSA plans to enforce such rights parameters.

3.3 ACCESS CONTROL

Are there protections in place to limit access to the digital trail of personally identifiable information created through the use of digital ID by both state and private actors?

While certain official limitations to the NPR data through the ID Act were discussed under "Actors", the realities of these controls does not seem positive. The DHA itself noted:

> *"The Identification Act and Alteration of Sex Description and Sex Status Act 49 of 2003, are key legislation that regulate how personal data that is hosted in the DHA identity management systems is handled. The legislation needs to be amended to regulate handling personal information in line with the Constitution and the POPI Act. The current practice of dumping the department's data on other government systems is contrary to the POPI requirements" (DHA, 2020).*

Interestingly, this implicates not only the practice of access, but also the cloud practices – reinforcing the relevance of the *Draft National Data and Cloud Policy*, 2021.

3.4 EXCLUSIONS

Are there adequate mechanisms to address exclusion from the system?

Perhaps unsurprisingly, a chief failing of concern in relation to the current NPR is the manner in which it can contribute to exclusion. The current system of

registration centres on registration from birth, but is associated to the status of parents, unintentionally resulting in (DHA, 2020; Singh, 2021):

> *"...vulnerable groups [facing] significant economic and social barriers as a result. This group includes people who did not acquire birth certificates at birth, children of non-citizens who were born in South Africa, those who are excluded or improperly documented for historical reasons such as the borderline communities and Khoisan people, and abandoned children [and non-binary persons]. The new system proposes that every birth in the country, irrespective of the status of the parents, must be registered. At birth, the biometrics of a parent must be linked to the birth certificate of a child."*

Children will then be required to be re-registered within the system at the age of five, with their biometrics in the form of fingerprints and iris and facial photographs also being taken.

Those exclusions are specific to the identification bureaucratic process, but risks of exclusion also arise in relation to *digital* identity. South Africa has comparatively high Internet penetration in contrast to many countries in the region (at over 50% Internet penetration and 84% mobile phone penetration, but with only 11% household penetration) (Gillwald & Mothobi, 2019).There are also significant dimensions of inequality in access across gender, location and education lines (*ibid*). This has real implications for identity management.

As ambitions in the South African public sector apparently grow for a grand plan "panopticon" of centralised, multi-function national identity (Breckenridge, 2005), it has to be noted that the foundations are already exclusionary. South African Smart ID cards, for example, are only available at some DHA offices (although mobile units are finally being rolled out – unsurprisingly as a response to the announcement of the local government elections) (Question to the Minister of Home Affairs - NW1176 | PMG, 2020). Additionally, they can be obtained now through certain banks that use the live capture system in-house (MyBroadband, 2020).

3.5 MANDATORY USE

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

As a foundational digital identity system, mandatory participation is largely assumed. Especially in South Africa (and certainly in other post-colonial African countries), visibility to the state as a mechanism for receiving social services and benefits is a profoundly important part of public service. Reticence in populations to "prioritise" individual notions of privacy may be a legitimate response to a

history of exclusion through invisibility to state systems, and this social reality is a peculiar history that must be understood in framing perceived privacy challenges in relation to identity (Razzano, 2021).

There is a caveat to this, however. In Annexure A of the ID Act, the phased roll out of the Smart ID cards is outlined, but the surrender of the green bar-coded paper ID is mandatory on the issuing of a new, or amended, identity application. The ID Act obliges all people that have attained 16 years of age to apply for an identity card. Additionally, the Regulations in relation to the ID Act (GNR.978 of 31 July 1998) in fact create a related criminal offence:

> *"11. Steps to ensure that person applies for identity card.—(1) [An officer acting in the service of the Department of Home Affairs who has become aware that a person has not applied for an ID card once 16]* shall request the person concerned in writing to apply for an identity card within 7 days from the date of such request at the nearest office of the Department.
>
> *(2) The request shall be substantially in the form prescribed in Annexure 9, and a copy thereof shall forthwith be delivered to the nearest office of the Department.*
>
> *(3) Any person who fails to comply with a request under this regulation shall be guilty of an offence and upon conviction punishable to a fine and to a period of imprisonment not exceeding 12 months" (Emphasis added).*

South African law frequently criminalises statutory non-compliance (even in relation to labour law. etc.). Whilst there is no indication that this offence is frequently enacted, it is an important flag for any campaigns that may seek to resist comprehensive digital identity initiatives.

RISK-BASED TESTS

4.1 RISK ASSESSMENT

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

Perhaps given the long history of biometrics in digital identity programmes within South Africa (Breckenridge, 2014), there is little indication of risk assessments being used in the design of policy or implementation – at least in the more modern understanding of risk assessments that are utilised in technology and AI design (Bhandari *et al.*, 2020; Crawford & Calo, 2016).

This is not to say that pre-emptive consideration of risk (or at least responses to risks as experienced) do not inform policy in the identity arena. For instance, fraud perpetrated by officials (a potential privacy harm) has been identified as key consideration:

> *"[The DHAs] Information Security Policy [incorporated] a model [that] was built around proactive risk assessment and risk management where all users responsible for registering and capturing births and identity related applications within the domain of the organisation, are assigned with biometric fingerprint authentication, to detect and hold users accountable for fraudulent activities (Question to the Minister of Home Affairs - NW445 | PMG, 2021).*

The DHA has noted that it is currently trying to enact identity, without an approved identity management framework. That is, the department is implementing identity and digital identity as empowered to do so by law, though without a political framework for doing so (DHA, 2020). There is a recognition by the DHA that this makes it challenging to manage privacy and security risks – and particularly "...the contemplated privacy impact assessments in terms of POPI, and the cybersecurity audits in terms of the Cybercrimes and Cybersecurity Bill" (DHA, 2020). Importantly, in its Draft Policy it enshrines as a specific sixth principle: "Protecting user privacy and control through system design" (DHA, 2020). It thus seeks to specifically enshrine in policy privacy-by-design principles, meaning that "...no action should be required on the part of the individual to

protect his or her personal data" (DHA, 2020).Both the Cybersecurity Bill[14] (though not yet law) and the POPIA mandate forms of risk assessment for the public sector. In the Regulations to POPIA, GNR. 1383 of 14 December 2018, Section 4 has described as a statutory obligation for all information officers within public and private bodies that they ensure that: "…a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information". However, the subsequent issued Guidance Notice from the IRSA did not provide clarity on a suggested scope for such assessments.

Additionally, there is little indication of mechanisms for addressing more exclusionary and discriminatory harms. Having an entrenched and justiciable human rights framework forms a form of a priori harm framework for the drafting of statute, by requiring that all law that is drafted be compliant with these rights, but it is of course not the same as an obligated assessment. Particularly in regard to decision-making in the digital identity field, risk assessments would be beneficial (Crawford & Calo, 2016). A broad prohibition against automated decision-making using personal data perhaps tries to pre-empt these challenges, yet that will surely not be sufficient, given the likelihood of AI's centrality to such functions. For interest's sake then, the POPIA in Section 71 prescribes:

> *"71. Automated decision making*
>
> *Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct".*

There is the possibility, however, that within "Codes of Conduct" provided for in the POPIA (which are Codes recognised by the IRSA that relate to specific sectors and industries), standards for processing may articulate forms of risk assessment that give better expression to potential exclusionary and discriminatory harms in the processing of personal data within the identity context.

14 The Cybersecurity and Cybercrimes Bill, 2017 was divide into a separate Cybercrime Bill and Cybersecurity Bill. The Cybercrimes Act was signed into law as Act 19 of 2020 in 2021.

4.2 PROPORTIONALITY

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

During the drafting of the POPIA, there were indications that consideration was had to how different types of personal information may have different levels of risk; an expression of the well provided caution that privacy has to be considered "in context" (Nissenbaum, 2009). Different standards for lawful processing are provided for different forms of information, with (in different ways) more significant standards of processing requirements for:

- Children's personal information;
- Information deemed to be "special personal information", which is information relating to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings; and
- Bank account information (for which specific criminal offences for unlawful processing are created).
- There are thus forms of proportionality assessment in the construction of data protection laws, even if absent from the ID Act.

CONCLUSION

South Africa has a strong human rights framework, which has given expression to some progressive laws – including the POPIA (though there are shortcomings to the law that are beyond the scope of this case). Also, a sophisticated statutory environment means that laws are not simply isolated – but rather exist within a framework of related laws like the ID Act, and multiple Regulations and Notices.

Additionally, digital identity is being implemented in a context of historical incorporations of biometrics (Breckenridge, 2014), but also one which recognises the social value of expanding identity, given historical exclusions.

Grand and expansive visions for centralised digital identity seem to suggest significant risks for mission creep, accountability challenges, etc. as these initiatives expand under the NIS. The POPIA will nevertheless provide an important mechanism for trying to create actionable rights for the protections of citizens' privacy. How exclusionary and discriminatory harms are best dealt with will rely on developments in administrative justice, as well as the potential sectoral roll-outs of industrial Codes of Conduct in relation to personal data management. However this plays out, there remains a need for reframing identity issues as human rights issues, and not merely an enabling step for digital economies.

Specific recommendations for policymakers:

- prioritise the implementation of unique identifiers;
- advance the privacy-by-design principles included in the Draft Policy;
- ensure the effective capacitation of the IRSA to help with identity oversight;
- ensure administrative justice as an access and recourse component of the emerging digital identity environment.

Specific recommendations for technologists:

- prioritise risk-based design;
- remain aware of administrative justice obligations in relation to public-private partnerships; and
- explore the expansion of well-designed decentralised identity in the advancement of service delivery across South African instances.

Specific recommendations for civil society:

- prioritise data protection awareness-raising across stakeholders; and
- provide a broad perspective of rights issues to identity management, which includes privacy alongside access to information and service delivery provision, etc.

REFERENCES

Question to the Minister of Home Affairs—NW445 | PMG, (2021) (testimony of Member of Parliament Arries). *https://pmg.org.za/committee-question/15730/*

Bhandari, V., Trikanad, S., & Sinha, A. (2020, January 22). *Governing ID: A Framework for Evaluation of Digital Identity*. *https://digitalid.design/evaluation-framework-02.html*

Breckenridge, K. (2005). The Biometrie State: The Promise and Peril of Digital Government in the New South Africa. *Journal of Southern African*, *31*(2), 267–282.

Breckenridge, K. (2008). The elusive panopticon: The HANIS project and the politics of standards in South Africa. *Playing the ID Card*, 39–56.

Breckenridge, K. (2014). *Biometric State. The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge University Press. *https://libcom.org/files/keith-breckenridge-biometric-state-the-global-politics-of-identification-and-surveillance-in-south-africa-1850-to-the-present.pdf*

Breckenridge, K. (2019). The global ambitions of the biometric anti-bank: Net1, lockin and the technologies of African financialisation. *International Review of Applied Economics*, *33*(1), 93–118.

Burchell, J. (2009). The Legal Protection of Privacy in South Africa: A Transplantable Hybrid. *Electronic Journal of Comparative Law*. *https://www.ejcl.org/131/art131-2.pdf*

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. *https://doi.org/10.1038/538311a*

Department of Home Affairs. (2020). *Draft Official Identity Management Policy* (Public Consultation Version). *http://www.dha.gov.za/images/PDFs/Draft_Official_Identity_Management_Policy_-_Gazette_Version_of_22122020.pdf*

Finn, M. (2013). AllPay Remedy: Dissecting the Constitutional Court's Approach to Organs of State. *Constitutional Court Review*, *6*, 258–272.

Gillwald, A., & Mothobi, O. (2019). *After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries* (After Access 2018: A Demand-Side View of Mobile Internet from 10 African Countries After Access: Paper No. 7 (2018); Policy Paper Series No. 5). Research ICT Africa. *https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf*

Question to the Minister of Home Affairs—NW1176 | PMG, Parliamentary Question (2020) (testimony of Member of Parliament Gondwe). *https://pmg.org.za/committee-question/14098/*

Government of South Africa. (n.d.). *Smart Identity Document (ID) card roll-out | South African Government*. South African Government. Retrieved 21 April 2021, from *https://www.gov.za/about-government/government-programmes/smart-identity-document-id-card-roll-out*

Lawyers for Human Rights. (2020). The extent of statelessness. Available on *https://static.pmg.org.za/210309Presentation_by_LHR_on_Statelessness.pdf*, accessed on 12 September 2021

McQuoid-Mason, D. (2014). Privacy. In *Constitutional Law of South Africa: Commentary* (2nd ed.). Juta.

Naude, A., & Papadopoulos, S. (2016). Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1). *THRHR*, *79*, 51.

Nissenbaum, H. (2009). *Privacy in Context*. Stanford University Press.

Razzano, G. (2020). *The public-private: A key legal nexus for South Africa's AI future* (Policy Brief No. 6). Research ICT Africa. *https://researchictafrica.net/publication/the-public-private-a-key-legal-nexus-for-south-africas-ai-future/*

Razzano, G. (2021). *Understanding the Theory of Collective Rights: Redefining the Privacy Paradox* [Concept Note]. Research ICT Africa. *https://researchictafrica.net/publication/concept-note-understanding-the-theory-of-collective-rights-redefining-the-privacy-paradox/*

Razzano, G., Gillwald, A., Aguera, P., Ahmed, S., Calandro, E., Matanga, C., Rens, A., & van der Spuy, A. (2020). *SADC Parliamentary Forum Discussion Paper: The Digital Economy and Society*. Research ICT Africa. *https://researchictafrica.net/publication/sadc-pf-discussion-paper-the-digital-economy-and-society/*

Singh, K. (2021, January 8). *Home Affairs proposes new identity policy*. IOL News. *https://www.iol.co.za/mercury/news/home-affairs-proposes-new-identity-policy-a7fc4211-fed0-4162-adf0-13f42d97c5e9*

BusinessTech (Staff Writer). (2021, January 27). South Africa wants a new ID system – but Home Affairs needs to fix long queues and IT failures first. *BusinessTech*. *https://businesstech.co.za/news/it-services/463728/south-africa-wants-a-new-id-system-but-home-affairs-needs-to-fix-long-queues-and-it-failures-first/*

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220.

Western Cape Government. (2021, March 2). *Applying for an Identity Document*. Western Cape Government. *https://www.westerncape.gov.za/service/applying-identity-document*

ANNEX I

NOTICE ON DIGITAL IDENTITY CARDS

GN 728 of 11 July 2013: Replacement of green, bar-coded identity documents with identity cards (*Government Gazette* No. 36648)

DEPARTMENT OF HOME AFFAIRS
(Section 25 of the Identification Act, 1997 (Act No. 68 of 1997))

I, Grace Naledi Mandisa Pandor, Minister of Home Affairs, acting in terms of Section 25 of the Identification Act, 1997 (Act No. 68 of 1997) ("the Identification Act, 1997"), hereby issue the following notice:

1. The Department of Home Affairs ("the Department") shall, effective from 18 July 2013, issue identity cards in terms of Section 14 of the Identification Act, 1997, replacing the green, bar-coded identity documents, to South African citizens and permanent residents who are currently in possession of validly issued South African green, bar-coded identity documents, and to the new applicants for identity cards, ("new applicants"), as well as to the applicants for duplicate identity cards ("replacement/re-issue").

2. From the 18th of July 2013, South African citizens and permanent residents who are currently in possession of the green, bar-coded identity documents, as well as the new applicants, shall be required to apply for the new identity cards in accordance with the roll-out programme referred to in the paragraph below.

3. The programme for the issue of identity cards is expected to be rolled-out by the Department over a period of 6 to 7 years, and will be implemented in the phases that will be communicated by the Department from time to time. The first phase of the roll-out programme is indicated in the paragraph below.

First phase of roll-out

4. The first phase of the roll-out of issue of identity cards will commence on the 18th of July 2013, and shall include a pilot project, with the issue of identity cards to the identified categories of citizens, at selected offices of the Department and/or service points as determined.

The broader public will be advised by the Department, from time to time, regarding the submission of application for an identity card in accordance with the phases determined.

Fees

5. The current Identification Act, 1997 regulations regarding fees in respect of an application for a re-issue of a lost, stolen or damaged identity document shall

apply in respect of an applicant whose identity document has been lost, stolen or damaged, and I shall, by regulation, prescribe the fees payable, if any, for the replacement of an identity document with an identity card, as well as any other fee in connection therewith.

Validity of green, bar-coded identity documents

6. Upon issue of the new identity card to an applicant, the green, bar-coded identity document, if the applicant had previously been issued with one, shall become invalid from the time of issue of the identity card, and the applicant must upon issue of the identity card issued to him or her, surrender to the Department, the green, bar-coded identity document for cancellation.

A green, bar-coded identity document validly issued to any person in terms of the Identification Act, 1997, and which has not been cancelled by the Department, and where the applicant or the person in possession thereof has not been issued with an identity card, as contemplated in this notice, shall, during the roll-out of the programme for the issue of identity cards, remain valid until a date that will be fixed by notice in the Gazette regarding the validity of green, bar-coded identity documents.

Once the programme for the issue of identity cards has been rolled out by the Department, and at least within 3 (three) years from the effective date of this notice, or soon thereafter, I shall, in terms of Section 25 (4) of the Identification Act, 1997, by notice in the Gazette, fix a date regarding the invalidity of the green, bar-coded identity documents, and upon such date, all green, bar-coded identity documents shall cease to be valid.

PROCESS

Registration for application for an identity card

7.1 During the roll-out phases of the programme, applicants shall be required to register for application for an identity card, at a nearest Home Affairs local office, service point, or mission abroad, as the case may be.

The registration for application for an identity card shall be made by the applicant, in the prescribed form, and contain the information as set out in this notice below.

Once an applicant has registered for application for an identity card, his or her details shall be recorded by the department, in the prescribed manner, and such details shall be verified against the population register and his or her application shall be processed by the Department, as prescribed.

Processing of an application in person by the applicant

7.2 After registration for an application for an identity card, the applicant shall be

requested by the Department to appear, in person, at an identified Home Affairs local office, service point, or mission abroad, as the case may be, for further processing and finalisation of his or her application.

Further instructions by the Department of Home Affairs

7.3 Despite the process above-mentioned or in addition to the said process, the Department may, where it deems necessary, advise and issue instructions to applicants regarding any information for submission of an application for an identity card.

Issuing of identity card

7.4 The Department shall issue an identity card to an applicant whose application for an identity card has be registered and processed by the Department in the prescribed manner.

Documents and information

7.5 When appearing in person at a Home Affairs local office, service point, or mission abroad, as the case maybe, for processing and finalisation of an application for identity card, an applicant shall be required to—

submit his or her green, bar-coded identity document for cancellation, providing that his or her identity document shall not be surrendered to the Department until he or she is handed an identity card; or

present his or her birth certificate issued in terms of the Births and Deaths Registration Act, 1992 (Act No. 51 of 1992) (for first time applicants); and/or

submit any information as prescribed;

confirm the correctness of his or her particulars in accordance with Sections 11 (2) and 12 and of the Identification Act, 1997;

have his or her photograph taken in the prescribed manner; and

have his or her fingerprints taken in the prescribed manner.

Registration information

The applicant shall provide the following information in the form for registration for an application for an identity card—

his or her full names and surname;

his or her identity number;

full physical and/or postal address; and

at least one contact number of applicant.

ANNEX II

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. ■