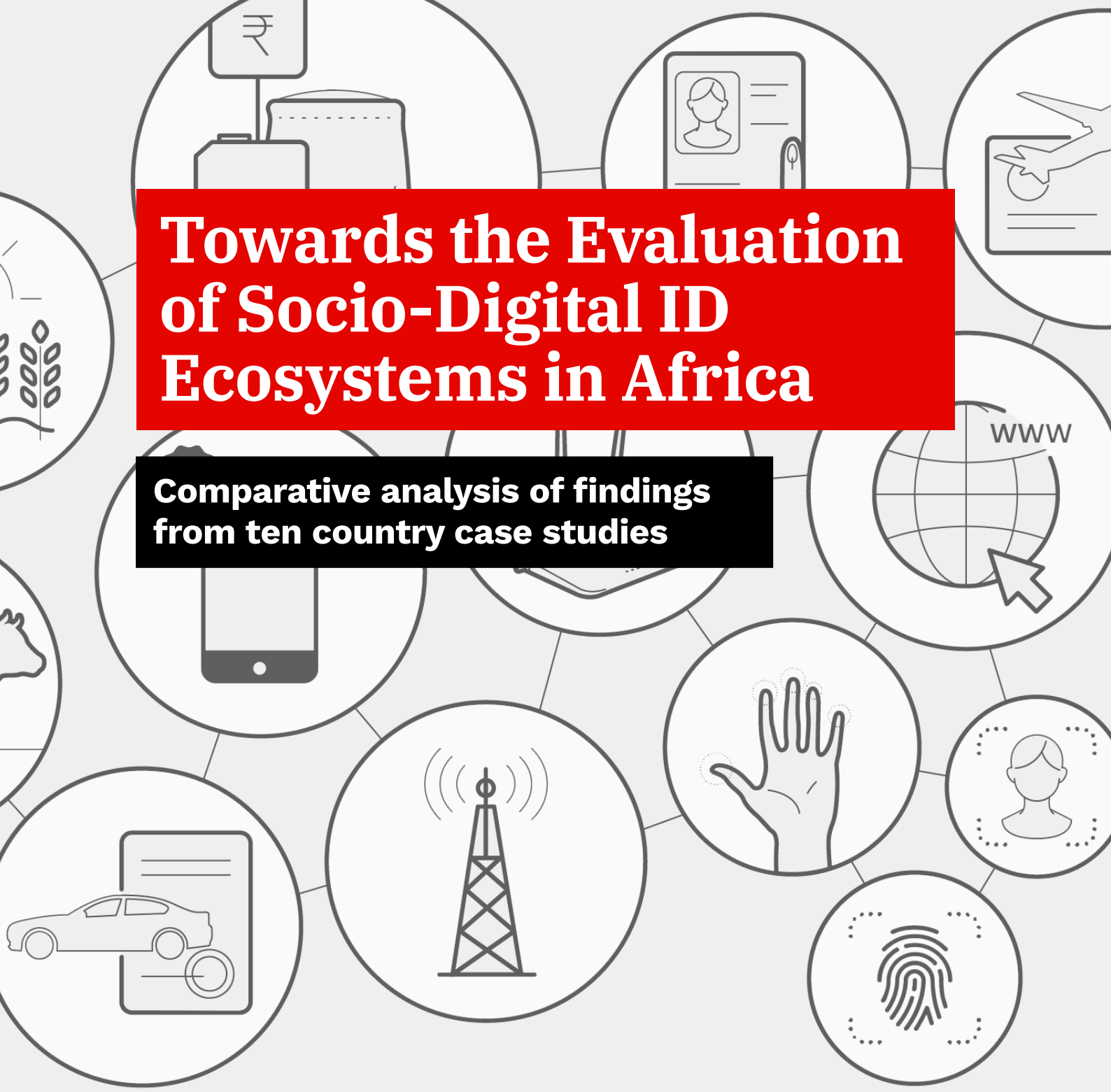

Towards the Evaluation of Socio-Digital ID Ecosystems in Africa

Comparative analysis of findings from ten country case studies

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

November 2021

REVIEW
Alison Gillwald, Amber Sinha, Kristophina Shilongo & Naila Govan-Vassen

EDITING
Samantha Perry & Ansie Vicente

COVER ILLUSTRATION
Akash Sheshadri

LAYOUT
Aparna Chivukula

RESEARCH ICT AFRICA

THE CENTRE FOR internet & society

OMIDYAR NETWORK™

Towards the Evaluation of Socio-Digital ID Ecosystems in Africa

Comparative analysis of findings from ten country case studies

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

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

Shared under
Creative Commons Attribution 4.0 International license

Towards the Evaluation of Socio-Digital ID Ecosystems in Africa

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

EXECUTIVE SUMMARY

Efforts to establish or improve national identification systems in Africa have coincided with the increasing deployment of mobile technology. This has led to the prioritisation of digital "solutions" for facilitating forms of identification and registration – often via biometric attributes.

With an estimated 500 million people in Africa living without any form of legal identification (birth certificate or national ID) (World Bank, n.d.), digital identities have become increasingly popular because of their relative ease, low cost, and convenience compared to more analogue systems. For example, the African Union Commission (AUC) is currently developing a digital ID policy framework for the continent. This effort draws its mandate from the Digital Transformation Strategy (DTS) for Africa (2020-2030), which highlights both the social and economic potential of digital IDs for Africans.

These implications are, if anything, underlined by COVID-19 (Martin, Schoemaker, Weitzberg & Cheesman, 2021) and the ways in which the devastating pandemic has tended to increase the utility of information and communication technologies (ICTs) on the continent and beyond (ITU, 2020a; Souter & Van der Spuy, 2021). Just like a pandemic can offer potentially compelling insights into socio-digital inequality, the state, and citizenship in Africa (Chigudu, 2020), digital identity ecosystems also proffer an interesting case study of development practices.

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 the state of digital identity ecosystems in 10 African countries. The project looked at local, digitised (in full or partially) foundational ID systems in Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe. The project set out to contribute to the broader question of whether digital identity ecosystems increase choices and opportunities for Africans, or whether they exacerbate the multidimensional aspects of digital inequality on the continent.

Critical analyses of the impacts and outcomes of digital identity ecosystems are important because related programmes tend to create an inherent power imbalance between the State and its people (and sometimes third parties with the deployment of public-private partnerships) because of the personal data such interventions collect. This leaves residents with little ability to exert agency in its collection, storage and use. And while increasing access to legal identification might appear on the face of it to be positive development processes, this is not always the case. In addition to the very real challenges of living without legal identification – whether digitised or analogue – those who do have digital identity sometimes face a range of other risks.

At the same time, digital identity ecosystems can be actively designed and shaped and therefore are not inevitably detrimental from a developmental, human rights, and/or inclusion perspective. Related policies might have a more transformative impact on the continent if they were conceived and designed with concepts like human rights, developmental goals, sustainability, and safety at the forefront, and if other inequalities are addressed alongside their implementation.

It is therefore crucial to continue to critically examine the design, development, and implementation of these evolving ecosystems. It is also important to assess whether policymakers are doing enough to ensure the positive outcomes of engagement with related technologies, while mitigating the risks that accompany these ecosystems on the continent.

The project

Ten African country case studies, which have been published as independent reports[1], informed this comparative report. While each of the countries have vastly different socio-political and economic digital realities to contend with, this comparative report aims to provide a synthesis of our general observations, the similarities and differences derived from our country partners' work, as well as recommendations for improvement and reform.

The research primarily took place within parameters set by the CIS's Evaluation Framework for Digital Identities, which was developed to assess how well digital identity systems comply with international rights and data protection norms. Certain aspects of the existing governance and implementation mechanisms of digital identity in the 10 countries were evaluated against the framework in these specific contexts.

1 See: Akuetteh Falconer & Odoru-Morfo, 2021; Mutung'u, 2021; Pule, 2021; Gaster & Martins, 2021; Okunoye, 2021; Binda, 2021; Razzano, 2021; Boshe, 2021; Iyer, 2021; Ngwenya, 2021.

A lack of a larger strategic vision seems to be a common theme in many countries, arising out of poor policy and legislative decisions and resulting in a crowded and disorganised identity management ecosystem. Many countries do not have either a digital ID or data protection legislation. Where such legislation does exist, it is often vaguely drafted, poorly implemented, or allows for significant executive discretion. The role of public and private stakeholders in this ecosystem remains opaque and poorly regulated. Significant apprehensions are raised around privacy and exclusion, particularly for already vulnerable and marginalised communities. This is amplified when digital ID is made mandatory, or at least effectively mandatory, to access vital government and private services.

Besides their specific responses to important questions in the framework, we highlight country partners' warnings about the lingering impact and significance of colonial systems of identity management on the continent. We also ask whether the digital identity frameworks now being promoted and lauded on the continent might expose Africans to new forms of (data) colonialism (Couldry & Mejias, 2019) as a result of novel systems of profitably extracting human experience and biometrics for socio-digital identities. We find that while many of the systems our country partners describe purport to be digital, they are often much more analogue in practice. In addition, many of our country partners warn that policymakers', development agencies' and development banks' adoption of digitisation as silver-bullet solutions, coupled with the "uneasy marriage between paper and digital systems" (Iyer, 2021), might lead to the neglect of, or even exacerbate, offline inequalities.

Another uncomfortable partnership is seemingly frequently forged between private and public sector stakeholders involved in constructing digital identity ecosystems on the African continent. In almost all of the countries surveyed, private actors had access to some part of the country's digital identity data, for example. In addition, many of our country partners also highlighted the lack of oversight and transparency as far as public-private interplays, partnerships, and procurements are concerned – especially regarding the fulfilment and delivery of technology related to digital identity ecosystems. The Ugandan and Zimbabwean reports, for example, raise concerns about opaque government contracts with foreign companies for installing or testing potentially problematic technologies (often including the risk of surveillance capabilities). There is often limited information about these partnerships and deals in the public domain and some contracts seem to barter national ID databases for technologies or infrastructure.

Another risk frequently highlighted in all the country reports is that of exclusion, albeit in different forms and guises in the countries surveyed. This multifaceted risk includes not just exclusion from identity digitisation processes (due to, for instance, low levels of Internet adoption) but also exclusion risks that are specific to the bureaucratic or administrative processes of identification.

When digital IDs are directly or indirectly mandatory for accessing a variety of benefits or services (as is the case in many of the countries examined), these risks tend to exacerbate socio-digital inequalities, often for those who can least afford it. Examples range from Nubian communities in Kenya, to the Njola (fingerprint-less) people in Uganda; the ancestors of the Gukurahundi massacres in Zimbabwe; some Fulani people in Ghana, and to many marginalised communities and intersectional groups, like women, elderly people, poor people, trans people, people in rural or remote areas, refugees, and migrants.

While it might be important for everyone to be legible to access critical services (Development Initiatives, 2021), marginalised communities, and data subjects more broadly, lack adequate protection and redress mechanisms. The country reports note that in some contexts, a plethora of actors and patchwork of rules apply or are relevant to digital identities. This not only leads to duplication and confusion, but often fails to adequately protect data subjects. Almost all of the case studies prompt calls for better policy and regulation to protect individuals' rights and offer better redress mechanisms.

While different contextual realities in each of the 10 countries examined mean different priorities and recommendations, we argue that the frequent similarities across the countries also means that countries could start by learning from the experiences of other African countries. Lessons can also be learnt from the broader ICT for development community, including, for example, that digital approaches to identity should always be accompanied by analogue options to avoid or mitigate exclusion risks. This includes phasing the introduction of such approaches and ensuring that there are always alternatives if digital approaches do not work (e.g., due to a lack of electricity or Internet connectivity).

Arising from these rich country evaluations, we recommend the use of more collaborative and multistakeholder approaches to the design, financing or funding, implementing and governance of digital identity ecosystems. A key priority should be actively including, in these collaborative approaches, the so-called beneficiaries of these systems, especially those who tend to be excluded from digital identity ecosystems. This is especially important as we find that many of the countries examined are currently in the process of reforming or creating policy instruments of direct or indirect relevance to digital identity ecosystems (e.g. South Africa, Zimbabwe, Mozambique, Lesotho, Kenya, and Rwanda). This presents an invaluable opportunity for civil society and other interested stakeholders to help shape a landscape in which digital identity can be more beneficial from a developmental, human rights and/or exclusion perspective.

Besides these general recommendations, the paper concludes with a detailed list of specific and distinct recommendations for policymakers, civil society, the technical community, private sector actors, donor agencies, and further research.

ACKNOWLEDGEMENTS

This project, consisting of the commissioning and overseeing of 10 country case studies and this comparative report, was made possible by the generous support received from Omidyar Network. This comparative overview paper was written by Anri van der Spuy, Vrinda Bhandari, Shruti Trikanad, and Yesha Tshering Paul, with the support of the Research ICT Africa and Centre for Internet and Society teams. The case studies referenced in this report formed part of an analysis of digital identity systems in 10 African countries, using an evaluation framework that was prepared by the CIS.

The country case studies were conducted by Teki Akuetteh Falconer and Smith Oduro-Marfo (Ghana); Grace Mutung'u (Kenya); Nthabiseng Pule (Lesotho); Polly Gaster and Iazalde Martins (Mozambique); Babatunde Okunoye (Nigeria); Elvis Mbembe Binda (Rwanda); Gabriella Razzano (South Africa); Patricia Boshe (Tanzania); Neema Iyer (Uganda); and Nhlanhla Ngwenya (Zimbabwe). Each of these studies were published separately and can be found at *https://digitalid.design/#africa* and *https://researchictafrica.net/category/research-papers-2021/*.

Peer review of this comparative report was done by Alison Gillwald, Amber Sinha, Kristophina Shilongo, and Naila Govan-Vassen. Editing was done by Samantha Perry and Ansie Vicente.

The authors thank the many people who made their time and expertise available to contribute to this report – especially the country partners.

ACRONYMS AND ABBREVIATIONS

AfCFTA	African Continental Free Trade Area
AU	African Union
AUC	African Union Commission
Bio	Biometric
CIS	Centre for Internet and Society
DTS	Digital Transformation Strategy for Africa (2020-2030)
GPS	Global positioning systems
ICT	Information and communication technology
ID	Identification document
MoU	Memorandum of Understanding
NIA	National Identification Authority (Ghana)
NICR	Department of National Identity and Civil Registry (Lesotho)
NIDA	National Identification Authority (Tanzania)
NIIMS	National Integrated Identity Management System (Kenya)
NIMC	National Identity Management Commission (Nigeria)
NIR Act	National Identity Register Act (Ghana)
NIR Regulations	National Identity Register Regulations (Ghana)
NIRA	National Identification and Registration Authority (Uganda)
POPIA	Protection of Personal Information Act, 2013 (South Africa)
RIA	Research ICT Africa
SDG	Sustainable Development Goal
The Framework	CIS Evaluation Framework for Digital Identities
UN	United Nations
UN SG	United Nations Secretary General

CONTENTS

OVERVIEW

1.1 BACKGROUND

With an estimated 500 million people in Africa living without any form of legal identification (birth certificate or national ID) (World Bank, n.d.), the provision of legal identity for all by 2030 (SDG 16.9) is an important goal in the United Nations' Sustainable Development Agenda (UNGA, 2015). Without a legal identity, many people are unable to participate in their societies and economies in a plethora of ways – from accessing healthcare or immunisation, to being eligible for cash or aid relief, or being able to vote. Women are particularly likely to be affected by identity divides: ID coverage among adults in Sub-Saharan Africa is reported to be almost 10 percentage points lower among women than among men (ID4D, 2017), for instance.

Efforts to improve national identification systems in African contexts have coincided with the increasing deployment of mobile technology, leading to some actors promoting digital "solutions" for facilitating forms of identification and registration – often via biometric attributes. Related digital identities have become increasingly popular since the 2015 Agenda because of their relative ease, low cost, and convenience compared to more analogue systems. The COVID-19 pandemic has, if anything, increased countries' appetite for digital identity platforms and technologies. As one recent report explains (Martin *et al.*, 2021):

> *Digital identity—already a fascination of government and aid actors for many years—has taken on a renewed significance during the pandemic, particularly as different initiatives are emerging internationally to leverage digital and mobile platforms for vaccine certification and immunity passports.*

Just like a pandemic can offer potentially compelling insights into inequality, the state, and citizenship in Africa (Chigudu, 2020), digital identity also provides a critical lens on development practices. In other words, do the technologies and platforms for digital identity increase choices and opportunities and enable Africans to "lead the lives they have reason to value", (Sen, 1999) or do they exacerbate inequalities – and often for those who are already marginalised?

A critical analysis of the potential benefits and risks of these systems and interventions is especially important because digital identities have recently been prioritised on Africa's policy agenda. For example, the African Union Commission (AUC) is currently developing a digital ID interoperability policy framework. The proposed framework aims at enabling "people in Africa to easily and securely access the public and private services they need, when they need them, and independently of their location" (AUC, 2021).

Among other policy instruments, this effort draws its mandate from the Digital Transformation Strategy (DTS) for Africa (2020-2030), which emphasises the significance of digitised legal identification mechanisms on the continent. The DTS highlights both the potential social and economic implications of digital identities for Africans. It notes that digital identities not only support social development, but also enable meaningful participation in processes to generate economic growth, spur innovation, and support entrepreneurship. In respect of the latter, digital identities are seen as critical for the successful implementation of the African Continental Free Trade Area (AfCFTA).

Some form of coherence and/or interoperability might indeed be beneficial, as African countries are at very different levels of development as far as foundational identity management is concerned. Some coherence is needed if they are to participate more equitably in the African common market. “Many countries are in intermediate levels of development, with coverage gaps among vulnerable populations and nascent digital capabilities,” the AUC notes. “Others have newly emerging or non-existent foundational ID systems.” While there is near universal coverage in countries like South Africa and Botswana, other countries suffer from much lower coverage levels. Almost 85% of African countries are reported to have national ID systems that are underpinned by electronic databases, and biometric data is collected in more than 70% of African countries (AUC, 2021).

At the same time, various multilateral agencies, global NGOs, and foreign donors are providing technical support as well as funding and loans for the deployment of digital identity roll-out across sub-Saharan Africa. Both foreign and local private sector actors are actively working to provide the relevant tools and equipment to implement these agendas in vastly different contexts. These actors commonly argue that digital identity can improve the efficiency of government payments and transfers; enhance the integrity of elections; improve financial sector services (via know-your-customer (KYC) and SIM registration); enhance public security; and promote safe and orderly migration (AUC, 2021). Benefits are said to extend to not only the public and private sectors (with digital identity offering valuable platforms for improving service delivery), but also to individuals (by enabling them to be visible to the state and to therefore become eligible for services).

With the growing appetite for digital identities across the world, there is a concomitant need to examine their impact on human rights, the rule of law, and social and economic inclusion or exclusion. While there have been some recent efforts to analyse the impacts of digital identities in countries like Uganda (Center for Human Rights and Global Justice, Initiative for Social and Economic Rights & Unwanted Witness, 2021) and Kenya (Schoemaker, Kirk & Rutenberg, 2019), examinations into the potential impacts and risks of ICTs are still relatively rare in Africa (and across the global South more broadly).

More critical analysis of digital identities' impacts in the global South, as well as the actors involved in designing and implementing it, is at least partly important because digital identity programmes create an inherent power imbalance between states and individuals because of the personal data such interventions collect. This leaves individuals with little ability to exert agency in its collection, storage and use. And while increasing access to legal identification might appear to be positive in development processes, this is not always the case.

In addition to the very real challenges of living without legal identification – whether digitised or analogue – those who do have digital identity might face other challenges. Experiences depend on context, 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 have IDs that are no longer fit for purpose in a digital age (AUC, 2021), while digitisation can introduce risks of exacerbating inequality when analogue options are discarded (especially in African contexts with low connectivity levels), as well as a plethora of other threats to human rights.

On the other hand, digital identity systems, like all information and communication technologies, are actively designed and shaped and therefore not inevitably detrimental from a developmental, human rights, and/or inclusion perspective (e.g., Lievrouw, 2014; Parikka, 2012; Freedman, 2002; Wacjman, 2000; Williams, 1985). In other words, there is hope: if digital identities are conceived and actively designed with concepts like human rights, developmental goals, sustainability, and safety at the forefront, they might yet hold a transformative impact for the continent (if other inequalities are addressed alongside their implementation and governance).

It is therefore crucial to continue examining evolving systems to ascertain whether policymakers are doing enough to ensure the positive outcomes of engagement with these technologies, while mitigating the risks that seem to accompany many digital identities on the continent. To do so, lessons can be learnt from the extensive work already done in developing an understanding of the outcomes of engagement with and exclusion from digital technology. For example, the development of and access to digital identity systems are faced with similar challenges to broadband adoption and digital ecosystems development (AUC, 2021).

1.2 THE PROJECT

With this background in mind, Research ICT Africa (RIA) and the Centre for Internet and Society (CIS) partnered to investigate, map and report on aspects related to the state of digital identity in 10 countries in Africa. The research took place within parameters set by an *Evaluation Framework for Digital Identities* (the Framework), which was developed by CIS with the purpose of assessing the alignment of India's digital system, Aadhaar, for compliance with international rights and data protection norms. It was subsequently used to assess a number of other digital identity systems in Europe, Africa, and Latin America. By using this Framework, partners evaluated certain aspects of the existing governance and implementation mechanisms of digital identity across different jurisdictions on the continent to determine if a particular application or use of digital identity meets certain criteria.

Ten country partners were asked to investigate local, digitised (in full or partially) foundational ID systems in Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe. The Framework they used to do so is built on a set of principles that are meant to target the many facets involved in a person being part of a national biometric ID programme or database. The Framework introduces a series of questions against which digital identity may be tested. It aims to address the various rights and freedoms that are potentially impacted by the state's use of a biometric digital identity programme.

The Framework begins with the assumption that the move from analogue to digital identity systems will, by definition, entail greater collection and generation of personally identifiable information, and result in greater privacy risks. In the past decade, several campaigns and litigations in countries, such as the UK, India, Kenya, and Jamaica have led to concerns about privacy, surveillance and exclusion. The Framework was designed as a ready guide for evaluation of ID systems.

The Framework takes a first principles approach and adopts three sets of tests: rule of law tests, rights-based tests, and risks-based tests, to assess the legitimacy and governance of digital identity in a specific context:

- The **rule of law** tests mandate that digital identity programmes must only be implemented within a legitimate regulatory framework that governs all aspects of the ID system, including its aims and purposes, the actors who have access to it, etc. These tests were largely intended to address the haste with which many digital identity programmes have been implemented, often in the absence of an enabling law which adequately addresses its potential harms.

- The second set of tests employ **rights-based** principles, such as necessity and proportionality, data minimisation, data subject rights to access, exclusion, etc., to evaluate the extent to which the rights of citizens might be infringed by using digital identity systems.
- Through the **risk-based** tests, the Framework assesses whether both the regulation and design of a digital identity system are sensitive to the potential risks that are likely to accompany this system. These tests focus on recognising the types of risks and related harms introduced by the different parts of an ID system (such as privacy harms, exclusion harms, and discriminatory harms) and implementing mitigation strategies and privacy-by-design systems to mitigate their prevalence and/or potential impact.

The Framework was designed by CIS to help inform the trade-offs that that must be made to build and assess digital identity systems or platforms to ensure that human rights are adequately protected. While more detail about the Framework can be found in Annex II, the next section contains a brief overview of the other conceptual underpinnings of the project.

1.3 CONCEPTUAL UNDERPINNINGS

Although practical in nature, this research project also drew upon a number of other theories and concepts that are important to define and examine. As noted, the project's overarching focus is the need to evaluate digital identity in the context of development in Africa. To do so, we drew upon Amartya Sen's understanding of development by asking whether digital identity technologies and platforms increase choices and opportunities and enable Africans to "lead the lives they have reason to value" (Sen, 1999), or whether they exacerbate socio-digital inequalities.

In respect of the latter, we also build upon RIA's body of research, which is geared to building an evidence-base for African decision makers and warns about the digital inequality paradox if states adopt technocentric solutions without attending to the underlying structural inequalities. To understand this concept, it is important to take a step back and look at the role of technology more broadly in the context of development.

ICTs, and specifically broadband technologies, have been identified as critical drivers of social and economic growth and development (e.g., UNGA, 2015). Smartphones, in particular, have significantly altered the telecommunications industry, and peoples' lives, by becoming the principal means of Internet connectivity in Africa. Similarly, the digitalisation of identification and registration systems is also often lauded for its developmental potential. But after years of sluggish Internet uptake with the high cost of fixed broadband services,

requiring expensive computer connectivity and relatively high digital literacy, the initial rapid mobile Internet adoption appears to have flattened out in many countries (c.f., ITU, 2020b).

RIA's After Access survey findings have shown that low Internet uptake is generally a result of challenges pertaining to human development (e.g., demand-side challenges like a lack of awareness or skills, or affordability). As a result, people at the bottom of the pyramid (often women and the poor) are most likely to be digitally marginalised or excluded. Some research into the impacts of digital identities on the continent has indicated that digital identities are also likely to exclude the marginalised or excluded (e.g., Center for Human Rights and Global Justice *et al.*, 2021). As Breckenridge explains in the South African context, specifically (2014:215):

> *...the price of [biometric ID] experiments was extracted from the poor over the course of the last century and they continue to pay today in the absence of institutions and infrastructure.*

This leads to the digital inequality paradox: as more people and things (including identities) are connected to the Internet, digital inequality seems to be increasing, not decreasing. This is not only the case between those that are online and offline, but those passively consuming what they are able to and those with the capabilities to put ICTs to productive use. As RIA has argued elsewhere (Gillwald & Mothobi, 2019), the digital inequality paradox is arguably the biggest challenge facing policymakers in an increasingly globalised economy over which they have limited control.

This project picks up on this notion by examining the impact of digital identities on development and asking whether they might ameliorate or aggravate socio-digital inequalities. The question is not necessarily polarised: digital identities can both recognise (on the positive end of the scale) and expose individuals to risks like surveillance, coercion or securitisation. As with other ICTs, expectations of digital IDs' nature and impact differ vastly, ranging from critical (even pessimistic) to optimistic (what some call "techno-utopian") (Helsper, 2021).

Rather than leaning towards one or the other, this project favours a critical view by drawing on materiality literature (e.g., Lievrouw, 2014; Parikka, 2012; Freedman, 2002; Wacjman, 2000; Williams, 1985). In this sense, digital ID systems are construed as actively designed and shaped, within significant historical and/or colonial contexts (Breckenridge, 2014). They are not inevitably detrimental from a developmental, human rights and/or inclusion perspective. The polarised views common in digital identity circles are, as others have argued, unhelpful and might even stunt deeper empirical analysis of and engagement with the realities of "so-called beneficiary communities" (Weitzberg, Cheesman, Martin & Schoemaker, 2021).

Conceptualising identity, identification and digital ID

This, finally, brings us to the definitions of (and the difference between) terms like **identity, identification, and digital identity** (Shilongo, 2021). Most systems on the continent have historically arisen in a non-digital or analogue domain, variously drawing on social and official conceptions of identity, identification and ID.

Our "identity" can be summed up as the relative social coordinates which distinguish one individual from another, meaning that identity is an ongoing negotiation. Non-digital identity is not fixed or absolute; it changes depending on the actors or the setting in which individuals find themselves. The process or transaction of proving unique identity is referred to as "identification", and at minimum this process requires two actors. ID is an acronym for identity or identity document in some areas. Contrary to identity, it is a credential which exists to authenticate participation in a certain identification system.

For legal identity within foundational ID systems as national identification systems, citizens interact with a national identity scheme or similar to access public services such as education, healthcare or protection. A citizen's identity is authenticated when they present predetermined basic characteristics such as their name, sex, time and place of birth to government officials. In most of the cases studies developed for this project, the identification process is supposed to begin at birth, when a birth certificate (also known as proof of legal identity) is issued to the individual as their unique identifier proving their existence; hence they have foundational national ID systems.

Besides foundational ID systems, other types of systems include sector-specific functional systems, such as a healthcare passport to access health services, or a voting card to exercise electoral rights. There are also modern-day systems designed to facilitate transactions across multiple sectors, with banking systems across Africa often being the most advanced form of transactional system.

As African societies are increasingly connected and digitalised (albeit in unequal ways), governments are adopting technology to achieve socio-economic goals by converting paper-based legal identities into digital data which can be more efficiently processed, stored and retrieved by machine systems. This process of digitalising legal identity results in what is known as a "digital identity". This concept is defined as any 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 (Nyst, Pannifer, Whitley & Makin, 2016).

In many African countries, the technology deployed is known as biometric (bio) technology. The system collects biometric data. This is defined as unique measurements of people's physical features, such as a fingerprint scan or scan of the eye's iris. The system can also collect behavioural characteristics such as one's voice. Although popularly used interchangeably, "digital identity" is distinct from digital ID. Although it is similar to the (non-digital) ID mentioned earlier, it is a digital artefact (i.e., a combination of characters, a unique number or barcode) used to authenticate one's digital identity. It can be derived from biometric technology, but digital IDs can also use other forms of electronic information (Nyst *et al.*, 2016).

1.4 LIMITATIONS

An important limitation of the research is that the country case studies were conducted using the analytical lenses provided by the CIS Framework, partly to assess whether the Framework is relevant in African contexts. The case studies and their findings might, therefore, not cover all aspects pertaining to digital identity in the respective contexts. At the same time, feedback from the country partners about what important questions the Framework might not have helped them answer, will help CIS revise and update the Framework to make it an even more relevant and useful tool.

The case studies represent the views and opinions of the country partners responsible for them (respectively), and do not necessarily represent the views of RIA or CIS. While RIA and CIS provided guidance to the country partners in using the Framework, and provided review and editing functions to the country partners, it did not check the findings or opinions expressed in the reports.

APPROACH AND FINDINGS

2.1 OVERVIEW

Given the need for more critical analyses of the impacts and outcomes of digital IDs in not only the global South, but specifically in Africa, the project tasked 10 different country partners – each with extensive local experience in their respective contexts – to assess digital ID environments in their countries using the Framework.

The researchers selected to conduct the country case studies come from different fields and disciplines, with only some having worked on digital identity projects before. The project therefore aimed to support local researchers in deepening their knowledge of digital identity, and in turn strongly benefited from having partners with different backgrounds and disciplines (from telecoms policy to administrative law, digital rights to data protection, journalism to women's rights, and more).

As mentioned, RIA purposefully selected a group of countries with different colonial histories, interesting contemporary challenges and socio-political environments, and diverse levels of broadband access/use. Some of the selected country partners mentioned the effect of having to contend with authoritarian governments; others with the devastating impacts of ongoing conflicts (e.g., Mozambique); many with the growing consequences of the climate crisis (e.g., Rwanda, Mozambique); and all with the impacts of COVID-19.

The 10 countries also have very different experiences and histories with identity management. For example, some of the countries have comparatively high levels of connectivity and ID coverage (e.g., South Africa), others low levels of connectivity but higher levels of ID coverage (e.g., Lesotho and Tanzania), and others with low levels of both connectivity and ID coverage (e.g., Mozambique). Some countries have been trying to develop or adopt digital identity schemes for a number of years (e.g., Nigeria), while others have only recently started discussions to develop more centralised or holistic digital ID systems (e.g., Mozambique). Some countries are further along this path of complex digitisation. South Africa, for example, is currently attempting to reform and modernise government identity management and align it with national development objectives through a draft policy recently published for public input, while Kenya has already experienced a court challenge pertaining to its third-generation identity cards (*Huduma Namba*).

The 10 countries examined for this project are therefore not directly comparable – nor was the goal ever for them to be – but the Framework allows for some comparison and contrasting against the evaluation criteria. In the

remainder of the section, we briefly discuss some of these similarities and observations – drawn from the country case studies – before turning to a more specific analysis of what the country partners found in terms of the Framework tests specifically.

2.2 GENERAL COMPARATIVE OBSERVATIONS FROM COUNTRY STUDIES

Many of the country partners commented on how the legacy of population control systems that commonly accompanied colonial regimes are still clearly discernible in contemporary approaches to (digital) identity.

Our Mozambique country partners, for example, describe a population identification system that started in colonial times to separate national citizens (indigenous or assimilated population) from colonisers (Gaster & Martins, 2021). In Zimbabwe, similarly, country partners describe a system of population control and registration that was inherited from a colonial regime, with its pillars "anchored in privileging the minority white settler community, while dehumanising and disenfranchising local inhabitants as well as black immigrants" (Ngwenya, 2021). In Kenya, similarly, the notorious *kipande* system (named after a piece of metal worn around the neck and containing identity papers) recorded the details of all African males over 16 years of age. It, however, relied upon British (colonial) interpretations and definitions of ethnicity and often erroneously categorised some clans, completely omitted others, and failed to account for the fluidity of ethnicity (Mutung'u, 2021).

These observations from country partners about the legacy of colonial systems are not surprising, given the established significance of biometric registration to "the ambitions of imperial progressivism" – already explored in depth in Keith Breckenridge's work. But – as Breckenridge also points out – it does compel us to be more critical about the ostensible promises, along with the perils, of digital forms of bio identification (2014):

> *There is a sweet and perplexing irony to the fact that those same coercive systems are now being championed as the only viable remedy to the entrenched forms of poverty that are characteristic of life in the former colonies.*

Such critical analysis extends to interrogating the risks that accompany these socio-digital identities, including the risk of extensive data extractivism. This, Couldry & Mejias (2019) argue, might amount to new systems of "appropriating" human life and making all aspects and layers of human experience the target of profitable extraction:

> *This extraction is operationalized via* data relations*, ways of interacting with each other and with the world facilitated by digital tools. Through data relations, human life is not only annexed to capitalism but also becomes subject to continuous monitoring and surveillance. The result is to undermine the autonomy of human life in a fundamental way that threatens the very basis of freedom, which is exactly the value that advocates of capitalism extol* (Couldry & Mejias, 2019).

Therein lies another irony, leading one to ask whether these colonially-rooted digital identity systems - in their guises of improving most aspects of life on the continent - might be introducing new and different forms of (data) colonialism.

While not really delving into such risks of datafication, many of the country partners question the value and impact of (identity) digitisation in especially colonial contexts. Grace Mutung'u (2021) laments in the Kenyan case study the "pouring of new wine (digital ID) into old skins (colonial ID)", explaining that there is a failure to address entrenched challenges and legacy problems when proposing "new" digital responses or "solutions". Her view is that the "main challenge" with Kenya's digital identity legal framework is that it tends to prioritise the introduction of technology "without resolving many other problems identified with the registration of persons law" (Mutung'u, 2021).

In Uganda, similarly, Neema Iyer (2021) reported that identity digitisation has been marred by the reality of trying to forge an "uneasy marriage" between paper and digital systems. This resulted in "a system that may be digital at its core but [that] is still mostly analogue on the periphery". While IDs in Ghana, on the other hand, have digital components, Teki Akuetteh Falconer and Smith Odoru-Morfo (2021) point out that "the alternative reimagination of the *Ghanacard* as a digital ID and not as physical cards is hardly present in the laws". As in other countries where identity digitalisation is not addressed in enabling legislation, they warn that in the case of Ghana, "...as digital components of the ID are increasingly used, the consequent peculiar dynamics and concerns around digital IDs are not specifically addressed in the ID laws."

In South Africa, policymakers' enthusiasm for digitising the identity ecosystem coincides with a more general appetite for the ostensible promises of the so-called Fourth Industrial Revolution (WEF, 2015). This means that opportunities for digitising existing identity management systems to facilitate trade, business and digital economy components are also lauded in a proposed identity management policy. However, as Gabriella Razzano (2021) argues in the South African country case study, such "ambitions for digital efficiencies" have to contend with the "reality of logistical failings through its own existing digital infrastructure".

In at least two of the countries investigated, these logistical failings include the practical considerations of having a plethora of sectors, departments, and

stakeholders involved in digital identity management. In Ghana, for instance, so many different types of state-issued IDs have proliferated over the years that the system has been described as a "card glut". This, in turn, introduces the risk that various state agencies managing certain aspects of digital ID maintain "a siloed approach as a way of retaining or hoarding the power and budgetary allocations associated with such ID projects" (Akuetteh & Odoru-Morfo, 2021).

The situation is similar in Mozambique, where the existence of a myriad of actors and a patchwork of activities relevant to developing (digital) identity systems across different sectors might potentially sacrifice the existence of any strategic or holistic vision, while also risking duplication and potential conflicts of interest. As Polly Gaster and Iazalde Martins warn (2021):

> *Due to the existence of many actors, coordination and leadership must establish a holistic vision of the future digital ID system and deepen the joint thinking about its goals, citizen rights, risk mitigation issues, the dangers of exclusion, practical implementation questions, and so on. There remains a risk that each actor ends up advancing in its specific sector, without having the opportunity to think through the strategic vision and the challenges and practicalities of implementation.*

The lack of strategic vision is also a failure of policy and legislation, a concern expressed in almost all of the country reports (e.g., Mozambique, Tanzania, Rwanda, and Zimbabwe). In Tanzania, for example, Patricia Boshe (2021) noted that while the country has expended many efforts to provide legal identity to all, there is a lack of "clear and sufficient rights protection and redress system" in the country. Not only do individuals lack the rules or procedural mechanisms to enforce their rights (the country lacks a comprehensive data protection framework), but officials responsible for rolling out digital identity systems are protected from prosecution if they mishandle data (Boshe, 2021).

In South Africa, despite the existence of the country's 2013 data protection legislation (which recently came into full operation), "grand 'panopticon' style centralisation of national identity ambitions" had emerged outside of and prior to the protections offered by data protection legislation (Razzano, 2021). The situation is similar in Mozambique (Gaster & Martins, 2021), where there is no specific law on digital ID, although the country is one of only eight African countries that have ratified the AU's Malabo Convention (which 14 countries have signed).[2] In the few cases where there are relevant policies in place, they sometimes suffer from being vaguely worded, as is reportedly the case in Nigeria

2 See: *https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf*.

(Okunoye, 2021).

On a more positive note, a few partners identified important policy windows that exist, with some countries in the process of reforming or creating policy instruments of direct or indirect relevance to digital identity ecosystems. At least some of these countries are also facilitating public deliberation or participation in these processes (albeit not always in the most proactive or direct of ways). This is arguably an invaluable opportunity for stakeholders to actively participate in, shape, and even help design a landscape in which digital identity can be more beneficial from a developmental, human rights and/or exclusion perspective. Potential opportunities include:

- In South Africa, the Draft Official Identity Management Policy was published in late 2020. While the deadline for public comments has passed, the process is worth following for subsequent opportunities for input, also in Parliament (Razzano, 2021);
- In Zimbabwe, the government has tabled a Cyber Security and Data Protection Bill before Parliament, and is reportedly currently receiving public input on it (Ngwenya, 2021);
- In Mozambique, both a data protection law and a national cybersecurity policy are currently being drafted and/or prepared (Gaster & Martins, 2021);
- In Lesotho, besides the need for establishing a functioning data protection regulator (in line with the country's existing data protection regulation), the draft Computer Crime and Cybercrime Bill awaits promulgation (Pule, 2021);
- Following a court case that challenged, among other things, the use of executive tools to make substantive changes to the existing national identity law, our Kenyan country partner calls for a new policy framework to be debated in Parliament, with more meaningful public participation and the inclusion of social interests (Mutung'u, 2021)[3]; and
- In Rwanda, a new law on data protection and privacy – reportedly posing significant implications for the digital ID landscape by containing a set of rights for data subjects and obligations for data processors – was published on 15 October 2021. As this development happened after the case study was finalised, its implications were not covered in depth but should be further assessed (Binda, 2021).

3 It should be noted that after the case study was already finalised, a High Court judgment ordered, among other things, that a data protection impact assessment would have to be conducted before the government could process any data or roll out cards. This development was not assessed in the case study.

While often under-regulated, one aspect that many of the country partners commented upon is the formal and informal interactions between private and public sector stakeholders. This concerns both the technical production of digital identity systems, and the access the private sector gains to public sector data on the basis of Memoranda of Understanding (MoUs). (As the latter is discussed in more detail in section 2.3 a) below, we focus on public-private partnerships here.) In Nigeria, for instance, Tunde Okunoye (2021) notes that attempts to develop digital identity systems have repeatedly been disrupted by corruption allegations around the public procurement of identity instruments (something that is reportedly also relevant in South Africa) (Razzano, 2021); a lack of technical knowledge transfer from a procured private sector company to public officials; and exorbitant costs (among other things).

The lack of transparency in many of these public-private partnerships makes scrutiny difficult. In the Ugandan case, for instance, a government contract with a Russian company (to install mandatory global positioning systems (GPS) trackers in all public and private vehicles) shows little concern for the potential impact that this development might still have on the digital identity ecosystem (Iyer, 2021). In Zimbabwe, similarly, Nhlanhla Ngwenya (2021) highlights the lack of transparency and public accountability in the context of the government's highly controversial partnership with a Chinese company (for rolling out a facial recognition programme).

Besides these privacy risks, another significant concern (explored in more detail in section 2.3 b) below) is the risk of exclusion. As with the digital inequality paradox, it is a risk that those that are already marginalised are more susceptible to. Our South African partner points out that the risk is two-fold: exclusions are not only specific to the bureaucratic process of identification, but exclusion risks also arise in relation to its digitisation. Besides the impact of low levels of Internet penetration in all of the countries surveyed (at approximately 54% Internet penetration, South Africa has the highest levels of access of the 10 countries) (Gillwald & Mothobi, 2019), inequality is intersectional and manifests across other dimensions like gender, location, tribe, culture, and education, for example (Razzano, 2021).

Fears of being excluded is a significant incentive for digital identity adoption or take-up (Boshe, 2021). Razzano explains that the desire to be visible to the state – especially in post-colonial African societies – should be understood in the context of identification often being a prerequisite for receiving social services and benefits:

> *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.*

Indeed, many of the countries examined make access to certain government services dependent upon having access to identity, meaning that digital identity becomes mandatory or *de facto* mandatory, even if the lack thereof is not criminalised (e.g., Ghana, Lesotho, Tanzania, Rwanda).

The need to have access to (digital) identity to access important public services not only incentivises adoption but increases the devastating impacts of exclusion (explored in detail in section 2.3 b) below). Most of the countries examined highlighted this risk for border communities, minorities (e.g., women, elderly people and the poor), and immigrants of colour.

Some undocumented Matabeleland people in Zimbabwe have said they feel like "they are 'stray animals' because they are undocumented" (Ngwenya, 2021). Similarly, in Uganda, Iyer notes that those who lack legal identity reportedly sometimes have to contend with the stereotype of being considered "suspicious and possessing criminal intent" (2021).

These risks are explored in more detail in the feedback to the Framework, discussed in the next section.

2.3 COMPARATIVE OBSERVATIONS IN RESPONSE TO THE FRAMEWORK

As mentioned in section 1.2 above (and in more detail in Annex II), the country cases are built around an assessment of the digital identity landscape in their respective contexts using the Framework, which lays out a series of tests to assess the legitimacy and governance of digital ID. This includes rule of law tests, rights-based tests, and risks-based tests.

In this section, the findings are presented as general observations, similarities and differences drawn from country partners' reports with regards to these three aspects of the Framework.

a) Rule of law

The rule of law tests evaluate whether an accessible and foreseeable legal framework regulates the use of digital ID in a country. Ideally, the roll-out of a digital ID system must be backed up by a validly-enacted law. Such a law should have a clearly defined purpose (to avoid mission creep) and should articulate the rights and duties of various public and private actors. Finally, the digital ID law should also put in place sufficient accountability measures to regulate the

actions of various actors, including by establishing adequate grievance redress mechanisms.

LEGISLATIVE MANDATE

Most of the countries surveyed as a part of this project (including Ghana, Lesotho, Mozambique, Nigeria, South Africa, Tanzania, and Uganda) have an enabling legislative framework to support the establishment of a digital ID system. Consequently, the agencies responsible for administering and implementing the digital ID project in these countries do have a statutory basis. However, there are some notable exceptions. For example, in Rwanda, while the national ID has a statutory basis, it does not extend to the digital aspects of the ID (Binda, 2021):

> *Digital aspects of the Rwandan ID are not regulated by the law. The law that provides for the issuance of national ID in Rwanda remains silent about the role of the NIN [National Identity Number] for online use, and the amount of information linked to one's NIN stored on the national ID database.*

Similarly, in Zimbabwe, the National Registration Act of 2011 regulates the issuance of the national identity card. However, despite sectoral use of digital IDs, there is no overarching national digital ID law or data protection law in the country that regulates the collection, storage, and use of personal and sensitive personal data for digital ID systems. As Ngwenya (2021) notes:

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

The Cyber Security and Data Protection Bill of 2020, which is currently pending consideration before the Zimbabwean Senate, seeks to plug some of these gaps, although Ngwenya (2021) identifies certain limitations with the Bill in his report.

Kenya's case is different from the other countries surveyed in this report. The enabling framework for Kenya's digital ID framework, the *Huduma Namba*, is found in a number of legislative acts. Firstly, there is an Executive Order (Executive Order No.1 of 2018); secondly, an amendment to the national identity law (Statute Law (Miscellaneous Amendments) Act, 2018); and thirdly, two sets of subsidiary legislation collectively referred to as the *Huduma Namba* Regulations (Registration of Persons (NIIMS) Rules, 2020 and the Data Protection (Civil Registration) Regulations, 2020) passed pursuant to the judgment of the Kenyan High Court on the legal basis of the digital ID project. Nevertheless, Mutung'u (2021) notes that

the *Huduma Namba* is being implemented without an overhaul of the existing law, and without addressing key issues of identification and exclusion, discrimination, oversight, and grievance redressal.

Concerns regarding the delegation of legislative powers to the executive depend on both the context and the country. Specific details regarding the delegation of powers to regulatory agencies and the role of the regulator in deciding policy questions about collection, storage, and implementation are contained in the individual country case studies that accompany this report.

In countries such as Ghana, Kenya, Lesotho, South Africa, and Uganda, the digital ID system is being rolled out alongside a national data protection law, although the latter is not always effective or implemented. In this regard, an important concern with respect to the accessibility of the law was pointed out by Nthabiseng Pule (2021):

> *...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. Sesotho is the native language spoken by about 90% of the population.... 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.*

In contrast, the law (Law 12/2018 of December 4) providing the foundation for e-SIRCEV (Electronic System for Civil Registration and Vital Statistics) in Mozambique is accessible to all citizens in physical and electronic form. In general, the law is freely accessible, although in some cases a nominal amount has to be paid for access. At the same time, however, the law is "extremely dense", with 387 provisions detailing every step of the process (Gaster & Martins, 2021). While such detailing may be necessary, it may also reduce the accessibility of the law for many citizens.

LEGITIMATE AIM

The countries surveyed for this project are divided in terms of whether the laws regulating digital ID contain an express or implied legitimate aim. However, in all cases, the aims behind the digital ID project can be deduced from a perusal of the title and provisions of the law, and the regulator's website (if one exists), as well as through government speeches.

Some common legitimate aims that seem to be present across countries include the need to:

- enhance social welfare;

- make e-governance and administration more efficient and digital-first, including by improving delivery and quality of public and private services;
- regulate the processes relating to the registration of persons. This includes issuing a national ID card, establishing and operating a national identification register, removing duplication from the registration process, and harmonising existing identification databases;
- improve national security, border security, and strengthening peace and security;
- curb the growing instances of crime and cyber-crime and preventing fraud; and
- boost economic development.

Our Tanzanian country partner observes that revenue generation is an under-discussed but important motivation behind mandatory registration of digital ID for accessing public and private services. For instance, the NIDA in Tanzania began charging all public and private entities Tshs 500 (approximately USD 0,22) per click/individual for using its services. This move has reportedly allowed NIDA's revenue to grow by 177% (Boshe, 2021). (The impact of mandating the use of digital ID for accessing public services is discussed in subsection b) below).

ACTORS AND PURPOSES

In almost all of the countries surveyed, private actors had access to some part of the digital ID data, either directly or through the respective government entity. There are three broad exceptions, however:

- In Mozambique, the e-SIRCEV system is not currently used or accessed by private actors for any general purpose (Gaster & Martins, 2021).
- In Rwanda, the national ID law does not expressly envisage the use of the national ID system by private actors. Despite this, as many as 45 institutions reportedly use the national identity number as a customer identifier, and banks and telecom companies have signed MoUs with the regulator to access the national ID database for KYC purposes (Binda, 2021).
- In Kenya, the Registration of Persons Act is silent on the use of the National Integrated Identity Management System (NIIMS) database by private entities. Nevertheless, national identity data can be shared with private entities in terms of other laws for purposes such as identity verification, car log books, and tax registration (Mutung'u, 2021).

Levels of regulation vary where private access to personal data is concerned, although many country partners have reported concerns around the misuse

of information by private parties and access to sensitive personal data for commercially exploitative purposes. For instance, in Tanzania, the authority, NIDA, gives public and private entities license through data sharing agreements to access the personal and sensitive personal data it holds. Details of such agreements are not in the public domain, and as such there is no clarity on whether private actors are granted access to the entire registry or only for verification purposes (Boshe, 2021).

Digital ID frameworks have been rolled out in most of the countries evaluated for a range of public and private services. Some of the common purposes across the countries surveyed include using digital ID for identification and verification purposes, registration of persons, verifying or updating voting registries, and providing social security, immigration, health, insurance, mobile, and banking services. In Uganda, the government shares its citizens' biometric data with telecom companies to facilitate the implementation of its compulsory SIM card registration mandate (Iyer, 2021). In Lesotho, South Africa, Nigeria, Tanzania, and Uganda, the ID framework is also used for public order and law enforcement purposes.

A concern arising from a number of the case studies is the lack of purpose limitation and the possibility of mission creep, discussed below, where the digital ID project gradually expands beyond its initial scope. This is more likely to happen in countries where the digital ID system does not have a clearly defined and limited purpose or where accountability frameworks are weak.

REDRESS MECHANISMS

Laws that regulate the implementation of digital ID systems must provide for adequate redress mechanisms against actors using these systems in case of data breaches, unauthorised or negligent sharing of data, or suspension or cancellation of ID. These redress mechanisms (and access rights) are often complemented by provisions in the data protection law of the country.

In Nigeria, the National Identity Management Commission (NIMC) Act, 2007 does not provide any avenues of redress for violation of the identity law. However, our country partner there feels that the gap might be plugged to some extent by Nigeria's Data Protection Bill (when or if it is passed) (Okunoye, 2021). In Mozambique, the Civil Registry Code does not provide any redress for violation of the law and citizens must avail remedies under different civil and criminal laws (Gaster & Martins, 2021).

With the exception of Lesotho and South Africa, it is not mandatory to inform users about any data breach, although public and private actors must inform the respective regulator of a breach. In South Africa, the Protection of Personal Information Act, 2013 (POPIA) imposes a positive obligation on public and private

actors to notify users of any data breach (Razzano, 2021). The Data Protection Act in Lesotho imposes a similar obligation, but redress mechanisms under the Act cannot be implemented since the regulator (the Data Protection Commission) is yet to be established (Pule, 2021).

Redress mechanisms also become important when a user's registration is cancelled, suspended, or withdrawn. Countries such as Kenya, Tanzania, and Uganda have established a framework (such as an administrative review mechanism) to hear the user before taking a final decision regarding such suspension or cancellation.

Most countries evaluated as a part of this report have some form of access and correction mechanism. In Lesotho, however, the correction mechanism is reportedly "onerous" and results in various unresolved grievances (Pule, 2021). In Uganda, the law authorises the National Identification and Registration Authority (NIRA) to correct any errors in the register or certificate. However, section 64(3) of the Registration of Persons Act imposes an obligation (rather than a right) on individuals to notify NIRA about any change or error in the recorded information. Failure to notify NIRA may lead to a fine and/or imprisonment (Iyer, 2021). At the end of the day, as our Ghanaian country partners note, the effectiveness of any redress mechanism will "always be shaped by citizens' awareness of their existence, and trust in the systems, in addition to judicial commitment" (Akuetteh & Odoru-Morfo, 2021).

ACCOUNTABILITY

Most of the countries surveyed reported low levels of accountability and transparency surrounding the operation of digital ID frameworks, especially regarding the use of personal data and sharing with third parties. South Africa stands out as an exception in adopting, at least on paper, a "subject-centred accountability framework" within the existing digital ID environment (Razzano, 2021).

As mentioned earlier, in Tanzania, the regulator, NIDA, is permitted to enter into private data sharing arrangements with third parties, with no obligation to provide any particulars of such agreements. Consequently, 45 data sharing agreements have reportedly been executed between NIDA and third parties. Unfortunately, there is no clarity surrounding the type and purpose of data being shared, or the period for which data shall be shared. The problem is exacerbated by the extensive and often unlimited powers given to the Minister to proscribe regulations (Boshe, 2021) (which is also the case in Zimbabwe) (Ngwenya, 2021).

In Rwanda, Binda (2021) identifies problems with the national ID database administrator (the National Identification Agency) playing the twin role of administrator and regulator of the database, and "the need for an independent

regulatory board that can hold NIDA responsible for any breach in the use or the management of the system". Similar concerns were expressed by Pule (2021) in the Lesotho country report, as the Department of National Identity and Civil Registry (NICR) simultaneously acts as an administrator of the register (responsible for data storage), as regulator (authorising third parties to access personal data), while also being involved in enrolments in the country. And in Nigeria, Okunoye (2021) notes that the law does not prescribe any system of accountability for the administrator of the ID system, the National Identity Management Commission.

Other concerns around accountability stem from a failure to prescribe penalties for non-compliance with various provisions, such as the duty of non-disclosure or the obligation to maintain information security practices. Kenya faces unique challenges due to the lack of accountability and clarity about the processes followed by the "vetting committees" that apparently assist with identification processes, mainly in border areas and areas where minority communities such as Nubians live (Mutung'u, 2021).

MISSION CREEP

Mission creep happens when there is gradual or incremental expansion of the digital ID project, beyond its original scope. This can happen for a variety of reasons ranging from no clear purpose limitation clause, interoperability frameworks, and weak legislative or judicial oversight mechanisms. Countries such as Nigeria have reportedly tried to curb the problem of mission creep by limiting technological access to the system through privacy and security policies (Okunoye, 2021).

In many of the countries surveyed, the problem of mission creep was due to the law containing broadly formulated purposes combined with significant discretion and power given to the concerned Minister/regulator to frame regulations in furtherance of such purposes. For instance, in Uganda, the Registration of Persons Act provides that government agencies may use the collected data for "related purposes". Using this provision, the Health Ministry in Uganda initially stated that only those with national ID cards would be able to access COVID-19 vaccines. The government only changed its position after significant public outcry (Iyer, 2021).

In Lesotho, the identification register may be used for purposes permitted under the National Identity Act, 2011 "or any other law". Once again, this creates "infinite possibilities" for the government to use citizens' personal identity data, without seeking a fresh mandate from Parliament (Pule, 2021).

Finally, in most cases, the law does not specifically criminalise or make provisions to prevent mission creep. In some cases, as in Kenya, the danger of mission creep arises from the government obtaining data from other sources, for humanitarian purposes, as in the case of double registration affecting Somali people in three counties in Kenya (Mutung'u, 2021).

b) Rights-based tests

It is critical for digital ID systems to be rights-respecting, particularly in light of their impact on privacy and freedoms and resulting exclusions. All country partners reported that the privacy violations from their respective digital ID systems were not proportionate to their purported benefits, and could not be considered just, fair, or reasonable.

DATA MINIMISATION

Most country partners reported that they found unclear limitations on the amount of personal data that can be collected, how this data is to be processed, and limits on retention. As noted above, Uganda collects vast amounts of sensitive information for registration purposes (including irrelevant information such as an individual's clan and ethnicity) (Iyer, 2021). Similarly, Ghana is said to collect more than 30 different data points about an individual, including height, eye colour and marital status (Akuetteh & Odoru-Morfo, 2021), a phenomenon also seen in Lesotho, with 23 data points collected (Pule, 2021).

In the country reports, it is noted that biometrics are often collected even when strictly unnecessary for use of the ID. In Kenya, for example, users are required to submit biometric information that would otherwise be considered deeply invasive, such as hand geometry, earlobe geometry, and voice waves, in addition to more commonly used fingerprints, and retina and iris patterns (Mutung'u, 2021).

In most cases, the seemingly extensive collection of sensitive personal data is carried out in the absence of explicit rules on data minimisation. South Africa is an exception to this, with data minimisation being a central principle of the POPIA. Here, too, the ID Act empowers the Department of Home Affairs to collect a broad array of data for the National Population Register, justified on the grounds of its civic functions. Our country partner argues that rules on data retention are either absent or vaguely articulated, and often left to the discretion of the executive (Razzano, 2021).

ACCESS CONTROLS

Laws limiting access control by public or private entities seem to be largely absent in the countries studied. Tanzania has no concrete legal framework for access

to identity data, although the NIDA is required by law to share data and create interoperability with other public institutions mandated to identify and register persons. The NIDA database is also linked to other public registries. A recent parliamentary report in the country found that NIDA had allowed no fewer than 41 private companies and 26 public institutions access to the NIDA database without the required documentation (Boshe, 2021). Similarly, Nigeria's NIMC Act also fails to provide sufficient safeguards to limit access (Okunoye, 2021).

In some instances, conditions for data access seem to have been left to the discretion of the executive. Uganda places minimal restrictions on data access. The purposes for which data may be accessed are open-ended and left to the Minister of Interior to prescribe (Iyer, 2021). In Kenya, the Data Protection (Civil Registration) Regulations require each civil registry to have access permission for management, documentation on security access as well as records of security incidents. However, the Regulations also leave it to each registry to develop its own protocols and do not provide principles on access controls (Mutung'u, 2021). Rwanda *prima facie* restricts access by public and private actors to the database. However, the Ministerial Order determining specifications of the national identity card and the fee related to national identification services makes a vague reference to getting "various services in public and private sectors" as one of the uses of the integrated smart card, but fails to specify how this should be done. This potentially opens up user data to many public and private institutions without a clear and binding legal framework (Binda, 2021).

While some of the countries that were reviewed have put slightly more stringent protection measures in place, these are generally inadequate. In Ghana, the Data Protection Commission, the National Identity Register Act (NIR Act), and the National Identity Register Regulations (NIR Regulations) together regulate access to identity data by user agencies. User agencies accessing ID information from the National Identification Authority (NIA) must show that the individual in question is aware of the authority of the asking agency, the purpose of accessing the information and the intended recipient. However, there is still an absence of explicit transparency around access rights and restrictions within the NIA (Akuetteh & Odoru-Morfo, 2021).

Lesotho, in turn, prohibits an unauthorised person from accessing the register or modifying information in the register, but may authorise third party access in accordance with instructions of the person to whom the information relates. A government department, statutory body or private entities can also access data for reasons of public order, public safety or public health. A specific provision is made for access by businesses whose activities are in sectors like 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. This, Pule (2021) warns, effectively allows many actors to access this

data in the absence of any oversight.

EXCLUSIONS

A recurring theme that emerged across the country case studies is the tendency to make digital IDs directly or indirectly mandatory for access to government and/or private services, without providing for alternative means of identification. This has led to exclusions. We see this in Nigeria, where the law mandates the use of ID for essential government services, such as opening a bank account or obtaining a passport, with no recourse in the absence of the required identification (Okunoye, 2021). Nigeria has thus made registration for digital ID to access essential services mandatory through the NIMC Act. Kenya has a long history of mandatory use of the national identity card. Despite this, the card is not available to every person, with research showing that people from border communities and ethnic minorities have reduced access to citizenship documentation (Mutung'u, 2021).

Uganda also mandates registration for digital ID. In addition to being unable to access services, a person faces criminal and administrative sanctions for failure to register. Anyone without a national ID cannot access several services, ranging from bank services to employment, insurance, pension transactions and any other type of service prescribed by the Minister. There is no justification for making ID mandatory in Uganda (Iyer, 2021).

We see similar tendencies in Ghana, Lesotho, Rwanda, and Tanzania, where digital identity is *de facto* mandatory.

In Rwanda, as Binda (2021) notes, the e-government portal Irembo – which users can only access using their digital ID – is increasingly being used to enable access to a multitude of public services, with no clarity on the legislative basis used to make the platform compulsory. In Tanzania, similarly, access to government employment and access to most public services is dependent on having an ID from the National Identification Authority (NIDA) (this seems to be on the basis of executive orders instead of parliamentary legislation). SIM cards must also be registered using the same ID, as Boshe (2021) explains:

> *As long as the Minister mandates the use of NIDA IDs in a certain sector, a service provider is justified in denying an individual service, in the absence of a NIDA ID.*

In Lesotho, as Pule (2021) notes, individuals:

> *...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.*

Ghana, too, does not officially mandate registration for national ID, although our country partners report that it is becoming *de facto* mandatory to access basic services (although alternative forms of ID seem to be allowed as well) (Akuetteh & Odoru-Morfo, 2021). Similarly, there is no mandatory requirement for use of digital IDs to access services in Zimbabwe (Ngwenya, 2021).

The tendency to require digital IDs for accessing public services does not take into account the many logistical, cultural or social factors that may prevent persons from enrolling for an ID, or successfully authenticating their identities.

OTHER EXCLUSIONS

As noted, low Internet penetration rates and a lack of stable electricity – among other infrastructural challenges – are barriers in many of the countries examined, causing widespread issues in enrolment and authentication. Additional issues arise from administrative or bureaucratic hurdles, or for sections of the population that are disadvantaged due to their remote locations (resulting in high travel costs), age (e.g., elderly people having incorrect information or degraded biometrics), sex (e.g., women not being allowed to leave the house, be photographed, or have their own ID cards), religious/ethnic identities or refugee status (e.g., minorities being excluded or deliberately persecuted on the basis of sensitive information).

In Uganda, for example, women are unable to access sexual or reproductive healthcare services without a national ID, and senior citizens who may not have fingerprints of sufficient quality are sometimes subjected to degrading remarks, as noted in a Parliamentary hearing (Iyer, 2021):

> *We have people who do not have [fingerprints]. In Luganda, we can call it "*Njola"*. Someone goes there with a thumb, most especially old people, they try to capture it and it cannot be captured. I have seen them being chased [away]. One time, I witnessed an old man being told to go and look for spirits [surgical alcohol], clean the place and come back. It was not even provided there but they told the old man to go away.*

In Zimbabwe, where a birth certificate is a prerequisite for national registration, our country partner reported that an estimated 300,000 people in the three Matabeleland provinces lack identification documents because their parents were killed in post-independence massacres of opposition supporters (the Gukurahundi massacres) (Ngwenya, 2021). Ngwenya (2021) further reports instances of failure to collect birth records from local health facilities in Zimbabwe, resulting in individuals having no birth certificate. Research indicates that some local clinics withhold birth records until mothers' maternity care fees are paid and related debts are cleared. When children are born at home or

outside formal health centres (e.g., in rural areas), parents are required to take along witnesses to registration centres to register their babies' birth. This is an added financial burden that is especially onerous for poor and rural families, as these witnesses typically have to be sponsored by paying for their travel to the registration centre, accommodation and food.

The cost of ID is also an important factor in exacerbating the risk of exclusions. While Rwanda has kept the costs of its ID very low (Binda, 2021), Ghana provides its citizens with a free ID (Akuetteh & Odoru-Morfo, 2021) but, an ID card for non-citizens costs USD 120, a figure that is prohibitively expensive for most. This is not the only challenge for non-citizens. In most of the country case studies, it was reported that refugees and stateless persons are routinely excluded from identity systems, with seemingly no attempt to mitigate these exclusions. For instance, Lesotho effectively excludes refugees from obtaining an ID (and provides no alternative means of identification), therefore locking them out of participating in the economy or accessing services despite the country being party to several treaties relating to refugees (Pule, 2021).

Very few countries have taken concrete steps to mitigate potential exclusions. An exception is Tanzania, which provides for the collection of alternative biometric information where the usual biometric markers are not recognised, and issues a certificate as temporary ID in case of loss of ID (Boshe, 2021). In Ghana, the National Identity Authority visited communities during its mass registration phase and is reportedly launching offices in all 275 districts in the country to reach rural and remote communities (Akuetteh & Odoru-Morfo, 2021). Most of the other countries examined lacked formal measures for reaching remote communities.

c) Risk-based tests

The risks introduced by a biometric national identity system are significant, and often not well accounted for by ID developers or policymakers. Our country partners found that although some of the risks inherent in an ID system were addressed by other rights-based and legal considerations, their governments rarely considered any risk identification or mitigation in their design and policymaking.

RISK ASSESSMENTS

To begin with, a publicly accessible risk assessment or framework was found in almost none of the 10 countries examined. An exception is Nigeria, where the National Identity Management Commission conducted a privacy risk assessment before the implementation of its digital ID project. The assessment was reportedly

comprehensive and accounted for the need for third party consent and the risks of the multipurpose use of the database, but failed to include other important risks such as that of exclusion (Okunoye, 2021). In Lesotho, the NICR allegedly conducted a risk assessment, but its outcome has not been published (Pule, 2021).

Some countries that have data protection laws may mandate a data protection assessment, but often digital identity projects are exempted from its application because it is done for the purpose of "national security", "public interest", or similar reasons. In the cases examined, risk assessments were either explicitly not done —as was admitted by the Kenyan government in court during the NIIMS case (Mutung'u, 2021) — or have never been published. Further, a data protection risk assessment is insufficient since risks of exclusion and discrimination, among other risks, must also be considered in a risk framework.

MITIGATING RISK

In addition to a risk assessment, it is necessary to have a governance framework that adequately addresses the risk involved in the use of a digital ID system. Often, the governing law accounts for the rights guaranteed by the country's constitution and other laws, but fails to address the inherent risks involved in a nationwide biometric system (in both its intended use and when it fails or is intercepted). For instance, the collection and use of inaccurate data has been known to have an exclusionary impact on ID holders using the system to access services, or otherwise prove their identity. However, most of the ID systems in the countries examined do not impose enough accountability on the administrators of the system, requiring instead that ID holders go through lengthy and inadequate recourse mechanisms (if any even exist). In Uganda, the governing Act has identified the high risk of inaccurate data collection to some extent, putting in place accountability measures for the verification of information and the correction of false information (Iyer, 2021).

Similarly, for other authentication errors, there was a noticeable lack of enforceable policy. Our partners in Uganda, Nigeria, and Ghana were unable to identify any regulation that addressed authentication errors, despite there being perceptible risks related to authentication in those countries. In Kenya, the Data Protection (Civil Registries) Regulations place accountability on entities using automated decision-making, applicable to authentication. However, there are no guidelines on how to mitigate against authentication errors, for example by using alternative methods of authentication, which are necessary to deal with exclusionary risks. During its 2013 elections, Kenyan election procedures were amended to allow for persons who could not easily be digitally authenticated to be physically authenticated due to authentication errors being experienced (Mutung'u, 2021).

Where the system itself fails, a properly conceived mitigation strategy can help to avoid mass exclusion, particularly when a society has come to depend on digital ID systems for access to goods and services. For instance, in September 2018, newspapers in Lesotho reported that the services provided by the NICR had been suspended because the company contracted to supply and operate the digital ID platform, had stopped working over non-payment of dues. Services also stopped in 2019 over non-payment of contract fees by the government (Pule, 2021). Instances like this are not uncommon, and contingency plans must be put in place to avoid disruption to a user's daily life.

None of the countries examined had a mitigation strategy for failure of the system in the ID Act. While Mozambique is implementing other cybersecurity policies that could address such situations, it was difficult to identify such frameworks in the other countries.

A well-implemented and effective data protection law is also necessary to address any gaps left by the governing ID law, while adding a second layer of accountability for digital ID administrators. This is lacking in Tanzania, Uganda, Rwanda, Mozambique, Nigeria, and Zimbabwe. In some cases, a bill has been introduced or passed, but the ID system still functions without a data protection framework. In some instances where a data protection law does exist, such as in Lesotho (Pule, 2021), the country does not have a regulator and said law therefore does not work effectively as an accountability measure.

CONCLUSION

3.1 OVERVIEW

As mentioned, the 10 African countries evaluated as a part of this project have vastly different contextual realities and these uniquely shape the practices and outcomes of digital identity in each. All of these African countries, however, contend with colonial histories that in different ways left legacies of identification governance (Breckenridge, 2014). These histories not only leave traces in contemporary approaches to (digital) identity management (and legacy legislation), but also influence citizens' desire for or reticence to being to be counted and recognised (Razzano, 2021; Development Initiatives, 2021).

These similarities also mean that countries could start by learning from the experiences of other African countries to address some of the challenges that impact the digital identity experience. At a time when quite a few of the countries examined have policy windows – i.e., where governments are working on developing legislation of direct or indirect relevance to digital identity (see section 2.2 above) – learning from each other (and not only from the foreign country examples often lauded by certain aid "partners") is especially important.

This brings us to the first of the recommendations. We start with some general recommendations before making specific recommendations for various stakeholder groups.

3.2 GENERAL RECOMMENDATIONS

Due to the multitude of stakeholders involved in implementing digital identity approaches, an overarching recommendation is to adopt multistakeholder, collaborative approaches in the development of digital and biometric systems to learn and benefit from the respective strengths that different stakeholders can contribute. Such participatory approaches are also important in ensuring that everyone involved in the conceptualisation, funding or financing, design, implementation, and governance of digital identity has a more holistic understanding of both the risks and the benefits of these interventions, as well as the need to prepare for them at all levels, from conceptualisation to governance. As Mutung'u (2021) notes in the Kenyan country case:

> *Digital ID is a complex issue that requires wide consultation and learning. Policymakers should not rush digital transformation. They instead should publish their digital ID plans and consider all input from other stakeholders, particularly those most likely to be affected by digital ID.*

Arguably the most important stakeholder category to be consulted in digital identity programmes is the so-called "beneficiaries" of these systems, including those who tend to be excluded. They are typically the people and communities that tend to be marginalised in socio-digital environments, for example women, children, elderly people, refugees, stateless people, people living with disabilities, people in rural areas, the poor, and less literate people.

With vastly different connectivity rates across the continent (Gillwald & Mothobi, 2019), coupled with different levels of "digital transformation" (and other inequalities), all of the surveyed countries have to consider analogue or less "digital" alternatives for identity management to avoid exacerbating socio-technical inequalities. In other words: digital approaches to identity must be accompanied by analogue options. This includes phasing in the introduction of such approaches and ensuring that there are always alternatives in the instances where digital approaches cannot work (e.g., due to a lack of electricity or Internet connectivity).

A number of the country partners also emphasised the importance of avoiding mandatory uses of national (digital) identity to mitigate the risk of exclusion (which affect marginalised communities most often). Many of our country partners made specific and useful recommendations for serving the communities that are commonly excluded in their unique contexts. In the Zimbabwean country case, Ngwenya (2021) made specific and useful recommendations to support women in the country, but many of these are more broadly applicable. They include the need for:

- formulating gender-sensitive policies which take into consideration the gender dimensions of access to documentation, to address gender disparities in registration, as women often bear the responsibility of registering children;
- prohibiting the withholding of birth confirmation records by health institutions and personnel for non-payment of hospital fees resulting in failure to register births essential for obtaining national IDs;
- using alternative supporting documents, such as health cards and affidavits, to address difficulties faced by women who give birth in areas where birth confirmation records might not be readily available;
- ensuring that birth registration laws encapsulate more contemporary trends in family structures to facilitate and enable registration by "non-traditional" parents;
- reviewing and developing application procedures and forms that take into account evolved family structures to allow family members to facilitate acquisition of national documents on behalf of children;

- conducting awareness campaigns to address cultural impediments which hamper access to documentation, such as the difficulties experienced by women who want to register children in their maiden names due to cultural beliefs that children must carry their father's surnames; and
- educating staff on the intricacies of the local communities they are operating in, to effectively provide the requisite services.

3.3 SPECIFIC RECOMMENDATIONS FOR DIFFERENT STAKEHOLDER GROUPS

While more specific recommendations tailored to specific country contexts are contained in each of the individual country case studies that accompany this report, some general recommendations can also be identified. For ease of reference, we divide them into recommendations for different stakeholder categories. Many of these recommendations are applicable across these stakeholder categories, however, and also in different phases of the development and implementation of digital identities. They are therefore not exhaustive and should not be read in isolation.

Recommendations for the public sector

Many of our country partners recommended that the governments and policymakers involved in the development of digital identities should consider more explicitly recognising national identity programmes as digital (rather than generic) identity programmes. This would allow them to adopt more direct approaches to digital technologies' specific challenges, risks, and implications. Similarly, in a few of the contexts examined, there appeared to be a tendency for some sectors to rely on forms of digital identity in the absence of any overarching legal framework to govern the use of digital identity.

To support these and related needs, a number of recommendations can be made for policymakers to develop or improve supportive legal environments by:

- developing dedicated policy instruments pertaining to the prevention, mitigation and resolution of risks pertaining to the digital components of national ID;
- advancing and entrenching privacy-by-design principles in policy instruments pertaining to digital identity;
- developing, adopting and/or implementing relevant policy instruments to protect and promote data subjects' rights as far as digital identity initiatives are concerned (e.g., data protection and cybersecurity legislation);

- translating relevant policy instruments to local languages, and using language that is less technical;
- ensuring administrative justice mechanisms as an access and recourse component of emerging digital identity environments; and
- ratifying the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), if they have not.

Given the aforementioned importance of collaborative and multistakeholder approaches to digital identity, these legal environments can only be developed following extensive and careful public consultations with all relevant stakeholders. These should include people or communities that are particularly at risk of not being served by digital identity. As Ngwenya (2021) points out in the Zimbabwe country report:

> *... there must be genuine public consultation to ensure citizens and all relevant stakeholders make meaningful contributions in the formulation of the law, which is essential in building trust between duty bearers and right holders in the application of the law.*

All of the case studies highlighted the risks of exclusion (along with its devastating impacts on affected communities). In addition to consultation, there is therefore a need for policymakers to take specific steps to safeguard the rights of potentially marginalised or excluded communities, including by:

- establishing mechanisms for the public resolution of complaints of exclusion;
- developing separate functions for distinct, independent regulators for data protection and privacy (e.g., an information commissioner or regulator), and (digital) identity management. The latter should have oversight over the licensing of agencies to perform registration and authentication responsibilities.

These regulators (and government actors more broadly) should assume proactive (and not merely reactive) stances to managing and governing digital identity, coupled with advocacy roles in raising awareness of privacy-preserving practices and mechanisms relevant to digital identity ID. Iyer (2021), in the Ugandan case, lamented the lack of awareness among Ugandans about how to protect their national identity numbers from being misappropriated and abused by third parties, and called for public awareness campaigns about how to safeguard digital identities.

When considering sharing identity data with the private sector, policymakers and the public sector should ensure that such sharing agreements only occur within the constraints of a specific MoU with suitable data safeguards, and that they:

- frequently and in accessible language(s) publishes the terms and conditions of MoUs, including the fees payable for access by private sector entities, terms of access, period of time, mechanisms implemented to safeguard data, and other costs involved;
- assesses the privacy concerns and other risks of sharing digital identity data with stakeholders from the private sector on a case-by-case basis;
- establish technical mechanisms for safeguarding data with the private sector, including the means of auditing access to and security of the data;
- foster transparency in granting access to digital identity information;
- conduct risk and human rights impact assessments before sharing digital identity data;
- consider the creation of data trusts to enable private sector entities access to certain non-sensitive identity data if they meet certain criteria, and establish a relevant oversight mechanism for setting standards and allowing safe access;
- mandate transparency and accountability by requiring external annual financial and risk audits and reporting to parliament.

Recommendations for the technical community

Because the design of technology has a fundamental impact on what affordances technology allow or disallow, the ways in which digital identities are conceptualised and designed are also fundamental. The roles and responsibilities of the technical community responsible for the design of digital identity architecture, are therefore crucial. Iyer (2021) points out that technologists have a similar responsibility to that of policymakers to develop codes and standards that ensure they develop "beneficial, responsible" digital identity interventions. She notes: "In today's digital society, it is extremely important for engineers and developers to work deliberately to implement and incorporate data protection and privacy guidelines into their code and products."

At the same time, and as Mutung'u (2021) points out, digital identities have outcomes and implications that extend far beyond the purely technical and should therefore be cognisant of contextual realities: "Any new technology developed and deployed should be sensitive to the nuances of the country and the situation to which it is to be applied."

Other recommendations from our country partners for those in the technical community, including stakeholders responsible for designing digital identities, can be summarised as the need to:

- design digital identity approaches that are suited to the target population, keeping in mind restrictions (e.g., a lack of electricity or Internet access) as well as the capabilities of target audiences;
- design approaches that embrace the data minimisation principle (i.e., only collect such data that are strictly necessary);
- adopt approaches that are not only safe-by-design, but also cognisant of potential risks;
- prioritise well-designed decentralised approaches, also to advance public service delivery;
- develop system architecture that takes into account issues of sustainability;
- work transparently and in a manner that prioritises the "explainability" of the workings of the technical infrastructure involved;
- develop system documentation to enable technicians and implementers to continually update and adapt system architecture; and
- remain aware of administrative justice obligations in relation to public-private partnerships.

Recommendations for private sector actors

While the recommendations for private sector actors, often responsible for financing digital identities, are similar and closely related to those for the technical community, additional recommendations include:

- taking necessary measures to ensure internal rules and regulations are developed that comply with customers' data protection and privacy rights;
- being transparent and publicly disclose any MoUs or similar legal agreements with public sector actors to facilitate access to identity databases; and
- working responsibly with data obtained from national ID databases.

Recommendations for donor communities

Specific recommendations for donor communities (including aid agencies), often responsible for funding the design, development and/or deployment of digital identities, include:

- ensuring that any projects or programmes are relevant to local contexts, and do not simply adopt foreign examples or "international best practice" for African contexts;
- prioritising working with local partners (as opposed to foreign experts);
- considering mandating multistakeholder participation in the development and implementation of digital identity programmes;
- supporting in-depth research and programmes not only about the digital ID but also about the country contexts of grantees;
- carefully understanding and specifying the intended beneficiaries of digital identity programmes, as well as assessing (and meeting) the actual needs of beneficiaries;
- investing in and understanding alternative and localised conceptions of digital ID; and
- investing in and understanding all potential outcomes of digital identity programmes, including the risk of collateral damage.

Recommendations for civil society actors

Many country partners felt that civil society actors could become more actively involved in digital identity debates, oversight and governance. As Binda (2021) argues with reference to the Rwandan context:

> *... given the propensity of the world to go digital, it is the responsibility of civil society to initiate research on the state of policies and laws regulating the use of digital ID in Rwanda in order to support the government. This will help to ensure that the government's vision to give Rwanda a paperless administration is not done to the detriment of people's constitutional rights and freedoms.*

Some country partners indicated that civil society organisations could benefit from working together more strategically on issues pertaining to digital identity. Civil society players traditionally concerned with issues of social justice should, for instance, work with and learn from civil society actors who work on digital rights. Mutung'u (2021) points out that such collaboration can play an important role in holding relevant stakeholders to account:

> *Digital ID policies for countries such as Kenya are driven by external forces such as development partners. However, their effects are felt by people who are either denied access to government services or experience these services differently. Civil society organisations have the task of bringing to the fore the effects of digital ID policies so as to influence better digital policy making.*

Similarly, one country partner pointed to the need for civil society actors to raise awareness of the importance of a range of rights beyond privacy rights, including rights to information and service delivery.

Civil society organisations can and should play an important role in monitoring and calling for relevant legislation and the independence of relevant institutions, like regulatory bodies, overseeing the implementation of digital identities. One country partner felt that donor agencies that promote digital ID interventions in Africa have a concomitant responsibility to "provide material and technical support to civil society organisations to deepen their interests and capacities on matters relating to ID systems, data and citizens' rights" (Okunoye, 2021).

To conclude, many of the country partners also recommended further research to better understand the outcomes, risks and opportunities of digital identities in their respective contexts – especially for communities that might suffer from exclusion due to a variety of factors.

REFERENCES

African Union Commission (2021). *Draft AU Interoperability Framework for Digital ID* (August, 2021). (forthcoming)

Akuetteh Falconer, T. & Odoru-Morfo, S. (2021) *Digital Identity in Ghana: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_Ghana.html* and *https://researchictafrica.net/publication/digital-identity-in-ghana-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

Bhandari, V. (2020a) *Governing ID: India's Unique Identity Program*. Centre for Internet & Society. Available at: *https://digitalid.design/evaluation-framework-case-studies/india.html*.

Bhandari, V. (2020b) *Governing ID: Use of Digital ID for Delivery of Welfare*. Centre for Internet & Society. Available at: *https://digitalid.design/evaluation-framework-case-studies/welfare.html*.

Bhandari, V., Trikanad, S. & Sinha, A. (2019) *Governing ID: Principles for Evaluation*. Centre for Internet & Society. Available at: https://cis-india.org/internet-governance/governing-id-principles-for-evalution.

Binda, E.M. (2021) *Digital Identity in Rwanda: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_Rwanda.html* and *https://researchictafrica.net/publication/digital-identity-in-rwanda-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

Boshe, P. (2021) *Digital Identity in Tanzania: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_Tanzania.html* and *https://researchictafrica.net/publication/digital-identity-in-tanzania-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

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

Cate, F.H. (2006). *The Failure of Fair Information Practice Principles* in *Consumer Protection in the Age of the 'Information Economy'* (Jane K. Winn ed.). Ashgate.

Center for Human Rights and Global Justice, Initiative for Social and Economic Rights & Unwanted Witness (2021) *Chased away and left to die*. Available at: *https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf*.

Chigudu, S. (2020) *The Political Life of an Epidemic: Cholera, Crisis and Citizenship in Zimbabwe*. Cambridge: Cambridge University Press.

Clark, J. (2019) *ID4D Practitioners Guide: Draft for Consultation*. World Bank. Available at: *https://responsiblefinanceforum.org/publications/id4d-practitioners-guide-draft-consultation/.*

Couldry, N. & Mejias, U.A. (2019). *The Costs of Connection: How Data is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press.

Development Initiatives (2021) *The Data Side of Leaving No One Behind* (discussion paper). Available at: *https://www.devinit.org/resources/data-side-leaving-no-one-behind/*.

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

Gaster, P. & Martins, I. (2021). *Digital Identity in Mozambique: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa. Research ICT & Centre for Internet and Society*. Available at: *https://digitalid.design/RIA_Mozambique.html* and *https://researchictafrica.net/publication/digital-identity-in-mozambique-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

Gillwald, A. & Mothobi, O. (2019) *After Access 2018: A demand-side view of mobile Internet from 10 African countries. Cape Town: Research ICT Africa*. Available at: *https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf*.

GSMA. (2019) *Digital Identity Country Report: Malawi*. Available at: *https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf*.

Helsper, E.J. (2021) *The Digital Disconnect: The Social Causes and Consequences of Digital Inequalities*. London: Sage.

ID4D (2018) *Data Note - ID4D Global Dataset and ID4D-Findex Survey*. Available at: *https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018-08/ID4D%20Data%20Notes%20revised%20082918.pdf*.

ITU (2020a) *Pandemic in the Internet Age: communications industry responses*. Geneva: ITU. Available at: *https://reg4covid.itu.int/wp-content/uploads/2020/06/ITU_COVID-19_and_Telecom-ICT.pdf*.

ITU (2020b) *Measuring digital development: Facts & Figures 2020*. Geneva: ITU. Available at: *https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx*.

Iyer, N. (2021) *Digital Identity in Uganda: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_Uganda.html* and *https://researchictafrica.net/publication/digital-identity-in-uganda-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

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*

Mutung'u, G. (2021) *Digital Identity in Kenya: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_Kenya.html* and *https://researchictafrica.net/publication/digital-identity-in-kenya-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

Ngwenya, N. (2021) *Digital Identity in Zimbabwe: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_Zimbabwe.html* and *https://researchictafrica.net/publication/digital-identity-in-zimbabwe-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

Nyst, C.; Pannifer, S.; Whitley, E.; & Makin, P. (2016). *Digital Identity: Issue Analysis*. Consult Hyperion. Available at: *https://chyp.com/wp-content/uploads/2020/06/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf*.

OECD (2013) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available at: *https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.*

Okunoye, B. (2021) *Digital Identity in Nigeria: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_Nigeria.html* and *https://researchictafrica.net/publication/digital-identity-in-nigeria-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

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

Paul, Y.T. (2020) *Governing ID: Use of Digital Identity for e-KYC in India*. Centre for Internet & Society. Available at: *https://digitalid.design/evaluation-framework-case-studies/ekyc-in-india.html.*

Pule, N. (2021) *Digital Identity in Lesotho: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_Lesotho.html* and *https://researchictafrica.net/publication/digital-identity-in-lesotho-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

Quijano, A. (2007). *Coloniality and modernity/rationality*. Cultural studies, vol. 21 (2-3):168-178.

Razzano, G. (2021) *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 ICT & Centre for Internet and Society. Available at: *https://digitalid.design/RIA_SouthAfrica.html* and *https://researchictafrica.net/publication/digital-identity-in-south-africa-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/*.

Schoemaker, E. Kirk, T. & Rutenberg, I. (2019) *Kenya's Identity Ecosystem*. United Kingdom: Caribou Digital Publishing, 2019. Available at: *https://www.cariboudigital.net/wp-content/uploads/2019/10/Kenyas-Identity-Ecosystem.pdf*.

Sen, A. (1999) *Development as freedom*. Oxford: Oxford University Press.

Shilongo, K. (2021) *Digital ID 101: Making sense of key terminology* (blog). Africa Portal. Available at: *https://www.africaportal.org/features/digital-id-101-making-sense-key-terminology/*.

Sinha, A. (2019) *Towards a Framework for Evaluation of Digital Identity: Draft for Discussion*. Centre for Internet & Society. Available at: *https://digitalid.design/evaluation-framework-01.html.*

Sinha, A. (2020) *Governing ID: Kenya's Huduma Namba Programme*. Centre for Internet & Society. Available at: *https://digitalid.design/evaluation-framework-case-studies/kenya.html.*

Sinha, A. & Saxena, P. (2019) *Research Plan*. Centre for Internet & Society. Available at: *https://digitalid.design/research-plan.html.*

Souter, D. & Van der Spuy, A. (2021) *Covid-19 Impact on E-Commerce: Global Report*. Geneva: UNCTAD. Available at: *https://unctad.org/system/files/official-document/dtlstict2020d13_en.pdf*.

Trikanad, S. (2020a) *Governing ID: Estonia's E-Identity Program*. Centre for Internet & Society. Available at: *https://digitalid.design/evaluation-framework-case-studies/estonia.html*.

Trikanad, S. (2020b) *Governing ID: Use of Digital ID for Verification*. Centre for Internet & Society. Available at: *https://digitalid.design/evaluation-framework-case-studies/verification.html*.

Trikanad, S. (2020c) *Governing ID: Use of Digital ID in the Healthcare Sector*. Centre for Internet & Society. Available at: *https://digitalid.design/evaluation-framework-case-studies/healthcare.html*.

Trikanad, S. & Sinha, A. (2019) *Digital Identities: Core Concepts and Processes*. Centre for Internet & Society. Available at: *https://digitalid.design/core-concepts-processes.html.*

Trikanad, S. & Sinha, A. (2019) *Holding ID Issuers Accountable: What Works?*. Centre for Internet & Society. Available at: *https://digitalid.design/rightscon-2019-report.html.*

UNGA (2015) *Resolution adopted by the General Assembly on 25 September 2015: Transforming our world: the 2030 Agenda for Sustainable Development* (A/Res/70/1). New York: UNGA.

Wacjman, J. (2002) Addressing Technological Change: The Challenge to Social Theory. *Current Sociology*, vol. 50(30): 347-363.

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.

World Bank (n.d.) *Global ID4D Dataset*. Available at: *https://id4d.worldbank.org/global-dataset*.

World Bank (2017) *Digital Identity Toolkit: A Guide for Stakeholders in Africa*. Available at: *https://www.id4africa.com/articles/DigitalIDToolkitforAfrica2014EN.pdf*.

World Bank (2019) *G20 Digital Identity Onboarding*. Available at: *https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf*.

World Economic Forum (2016). *The Fourth Industrial Revolution: What it is, how to respond*. Available at: *https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/*.

ANNEX 1

RIA'S WORK ON DIGITAL INEQUALITIES

Research ICT Africa (RIA) is a digital policy think tank with an extensive footprint across Africa. It has two decades of experience working with African governments, the African Union Commission, regional economic communities, and multilateral organisations on policy formulation, regulation and governance.

In support of global initiatives to develop universal indicators and to ensure that they are appropriate for developing countries, RIA has also worked extensively with international agencies such as the International Telecommunications Union (ITU), the United Nations Commission on Trade and Development (UNCTAD), the Organisation for Economic Co-operation and Development (OECD), and various national governments to collect up-to-date data, particularly demand-side data.

Some highlights of our recent work include:

- In South Africa, RIA led the public consultation and drafting of the South African national broadband plan, SA Connect, for the Department of Communications. This effort was acclaimed by the UN Broadband Commission on Sustainable Development.
- RIA was commissioned by the African Development Bank and the Government of Mauritius for one of the first integrated digital economy plans on the continent, i-Mauritius.
- RIA has also developed and continues to operate an African transparency pricing portal that produces the RIA African Mobile Pricing Index, a pricing touchstone for African regulators and competition authorities. The Index is unquestionably the most quoted and influential pricing and affordability barometer on the continent and is used widely by UN organisations and development banks.
- RIA was commissioned by the African Development Bank to develop a new data protection model law for the Southern African Development Community (SADC) in 2019. It is currently developing a digital economy model law with the SADC Parliamentary Forum as part of an IDRC-funded capacity-building and knowledge-transfer initiative.
- Together with its sister networks in Asia (LIRNEasia) and Latin America (DIRSi), RIA has produced longitudinal and rigorous research at the national or sub-national level. For many countries, the RIA sector performance reviews, and access and use surveys provide the only public domain data and analysis of the progress being made towards reaching public policy objectives.

As a result of these and other projects, RIA enjoys high levels of credibility among donors and has a reputation for excellence, delivery and accountability. RIA has built enduring relationships with donors that include the Canadian International Development Research Council, Department for International Development, Open Society Foundation, Google, and the Shuttleworth Foundation.

INTRODUCTION TO CIS' WORK ON DIGITAL ID IN INDIA

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The research at CIS seeks to understand the reconfiguration of social processes and structures through the Internet and digital media technologies, and vice versa. Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and regulatory practices around the Internet, technology, and society in India, and elsewhere.

CIS has been engaged into research about India's national digital identity project, Aadhaar, since its inception in 2009. A number of technical and policy solutions recommended by CIS - such as virtual identity and guidelines for handling of Aadhaar Numbers and related information by

government departments - have been incorporated into regulation by the Unique Identification Authority of India (UIDAI). Since 2015, CIS has been actively researching big data in the global South, with digital identity as one of the key drivers of big data generation. Since 2019, CIS has worked on its Framework (Governing ID: Principles for Evaluation), conducted systems mapping to identity systems in different parts of the world, investigated how courts understand identity systems, and enquired how an inclusive, privacy-preserving technological and policy design of identity systems can be determined.

ANNEX II

OVERVIEW OF FRAMEWORK

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

The impetus for this document came from Clause 16.9 of the UN Sustainable Development Goal (SDG), namely: "By 2030, provide legal identity for all, including birth registration" (UNGA, 2015). While the UN SDG only calls for legal identity, countries across the world have begun implementing new, foundational, digital identification systems ("digital ID"), or begun to modernise their existing ID programmes.

The history of digital ID programmes in countries such as India, Kenya, Estonia, Jamaica, and the UK demonstrates 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 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 Framework for digital ID. CIS (Sinha & Saxena, 2019) 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" (Nyst *et al.*, 2016). 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" (Clark, 2019).

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 (OECD, 2013), and international scholarship on harms-based approaches (Cate, 2006).

RULE OF LAW TESTS

Digital ID systems 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,[4] 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 (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.

4 A validly enacted law has three components: (i) it should be passed by the Legislature, and not the Executive; (ii) it should be accessible and foreseeable — this is to ensure the "quality of law"; and (iii) it should be clear and precise — this is to limit the scope of discretion.

RIGHTS-BASED TESTS

Criticism of digital ID systems focuses 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 by digital ID systems. These tests ask five questions about:

1. Necessity and proportionality – whether the privacy violations arising from the use of digital ID are 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 to personal and sensitive personal data by state and private actors controlled through the law.
4. Exclusion – whether there are adequate mechanisms to ensure that the adoption of digital ID does not exclude citizens and/or 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 (such as privacy harms, exclusion harms, and discriminatory harms) caused by its uses, 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 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 Framework, CIS published case studies on the use of digital ID for the delivery of welfare (Bhandari, 2020b), for verification (Trikanad, 2020b), and in the health care sector (Trikanad, 2020c). Country specific case studies were carried out for Estonia's e-Identity programme (Trikanad, 2020a), India's e-KYC framework (Paul, 2020), India's Unique Identity (Aadhaar) programme (Bhandari, 2020a), and Kenya's *Huduma Namba* programme (Sinha, 2020).

The eventual aim of the 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.

ANNEX III

METHODOLOGY

RIA selected a sample of countries with different developmental agendas, different institutional histories, and potentially colourful experiences with digital ID, namely Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe.

Thereafter suitable country partners were selected with relevant expertise or experience in research and/or policymaking pertaining to digital technologies in development contexts in general, and digital ID more specifically. In certain instances, we opted to work with partners with longer experience in information and communication technologies (ICTs) in development contexts, in data protection and privacy, but less experience in digital ID specifically. The selected country experts were:

- Ghana: Teki Akuetteh Falconer and Smith Odoru-Morfo (Africa Digital Rights Hub)
- Kenya: Grace Mutung'u (Centre for Intellectual Property and Information Technology Law, CIPIT)
- Lesotho: Nthabiseng Pule (Cybersecurity Capacity Centre for Southern Africa, C3SA)
- Mozambique: Polly Gaster and Iazalde Martins (Centro de Informática Universidade Eduardo Mondlane, CIUEM)
- Nigeria: Babatunde Okunoye (Berkman Klein Center/Paradigm Initiative)
- Rwanda: Elvis Mbembe Binda (University of Rwanda)
- South Africa: Gabriella Razzano (RIA/Open Up)
- Tanzania: Patricia Boshe (African Law and Technology Institute, AFRILTI)
- Uganda: Neema Iyer (Pollicy)
- Zimbabwe: Nhlanhla Ngwenya (Independent/MIISA)

These country partners' profiles and brief biographies are contained in Annex IV to this document.

RIA and the CIS team hosted two training workshops on consecutive days to familiarise partners with the Framework. The CIS team primarily led these workshops by going through the Framework and discussing other use cases of it

(e.g., Estonia). Partners were given reading material (the framework and other use cases) beforehand.

After the workshops, RIA and CIS continued to host fortnightly meetings with all partners to check in on status and to learn from experiences. To enable partners to get to know the Framework better, they were asked to prepare for using a specific aspect of the Framework before each meeting, including first assessing the availability of functional or foundational systems in the country concerned, gathering data for the rule of law test, the rights test, and the risks test respectively. Potential challenges were addressed during these meetings, and partners were also given an opportunity to learn from how other partners had overcome challenges (such as where there was a lack of relevant data available).

First rough drafts of the country case studies were due by 30 April 2021. These drafts were reviewed by both the CIS and the RIA teams, along with peer partners. Each draft was thus reviewed at least three times, and constructive feedback was given to the partners to help them strengthen (where applicable) their work.

Partners then revised and completed their case studies on the basis of the feedback given, and submitted it for peer review. In some cases, case studies received significant suggestions for changes but partners had the opportunity to liaise with peer reviewers to learn from feedback. Finalised drafts were completed in July 2021 before the case studies went for proofreading and layout.

On the basis of the completed reports, a comparative synthesis report was prepared by the CIS and RIA team.

To work towards the creation of the State of ID Africa website/portal, each partner was asked to write an informal, conversational blog or opinion-editorial that can be used on the portal, in addition to their more academic case studies. RIA also conducted a “spotlight on” interview with each partner to introduce partners to the audience in a more informal manner. The questions used for the interview were rather informal and conversational, and featured on RIA’s website. A large selection of the blogs were featured in a special edition (Digital ID Dispatches) on Africa Portal.

ANNEX IV

COUNTRY PARTNERS

GHANA

Teki Akuetteh Falconer is the Founder and Executive Director at the Africa Digital Rights Hub. She was the first Executive Director to set up the Data Protection Commission of Ghana and facilitate implementation of Ghana's Data Protection Accra until her exit in July 2017. She is a privacy and data protection consultant and has previously worked for the Government of Ghana in the development of several key legislations. She has worked in various capacities with regional bodies such as ECOWAS. She is a member of the UN Global Pulse Privacy Advisory Group, the UN Special Rapporteur for Privacy Taskforce on Health Data Privacy, and serves on the advisory committee for the 40th International Conference of Data Protection and Privacy Commissioners. She holds an LLM in Information Technology and Telecommunications Law from the University of Strathclyde, Glasgow, Scotland, and a Bachelor of Arts in Law and Political Science from the University of Ghana (Legon).

KENYA

Grace Mutung'u is an advocate of the High Court of Kenya and research fellow with the Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University. Her research interests are in ICT policy in Kenya and Africa, with a specialisation in digital rights, governance and development. She has been involved in ICT policy processes for over 10 years.

LESOTHO

Nthabiseng Pule is the Project and Outreach Manager for the Cybersecurity Capacity Centre for Southern Africa. She has a background in ICT and has experience working in ICT operations, universal access projects and ICT policy formulation. She started her career in ICT at the Central Bank of Lesotho 1998 as a business analyst. She then joined the Lesotho Communication Authority (LCA,) where she was the ICT manager for about 10 years, after which she took up the role of executive head responsible for universal access. She holds a Master of Information Systems, a Bachelor of Science in Computer Science and Statistics, a Postgraduate Diploma in Financial Management, and a Certificate in Telecommunications Regulation.

MOZAMBIQUE

Polly Gaster is a communication specialist. She has been working at the Eduardo Mondlane University Informatics Centre (CIUEM) since 1998 in the field of ICTs for Communication and Development. She was part of the Mozambican team that established the first telecentres in rural areas in 1999, followed by continuing community radio and community multimedia centre initiatives. In addition to activities on the ground in defence of citizen rights to information and freedom of expression, she has been active at national level in contributing to and commenting on legislation in the area, ranging from the Press Law of 1991 to the Right to Information Law, and more recently various ICT laws and regulations from a citizens´ perspective. She was a member of the African team that developed the African Declaration on Internet Rights and Freedoms.

Iazalde Martins holds the position of coordinator of the Community Information and Communication Support Center (CAICC), which was established by the CIUEM. He has a degree in Computer Engineering from the Higher Institute of Science and Technology of Mozambique (ISCTEM). He has worked at CIUEM since 2009, firstly as a technician and, since 2012, in CAICC, where he has served successively as Helpdesk Manager, Manager of the Olavula citizens platform. As coordinator at CAICC, he plans, budgets and supervises the execution of all activities.

NIGERIA

Tunde Okunoye, based in Lagos, Nigeria, is a researcher on digital society, particularly in the context of the global South. His research focuses on ICTs for development (ICT4D). He is a Fellow with the Berkman Klein Centre for Internet and Society, Harvard University, where his research focuses on the use of aggregate search engine queries to inform public policy and international development, particularly in statistically poor contexts of developing countries. He blogs on Medium (Tunde Okunoye @developmentmusings).

RWANDA

Elvis Mbembe Binda is a human rights advocate who works with Initiatives for Peace and Human Rights (iPeace) to enhance the culture of peace in the African Great Lakes region through human rights and good governance education. Through various projects that he coordinated, he has accumulated experience in working with grassroots people in remote rural areas and local leaders to address multiple ranges of human rights issues including expropriation, access to land, family disputes, and the like. His interest was recently piqued about issues related to digital ID as a result of the increased use of online services in Rwanda, especially since the outbreak of COVID-19.He holds a PhD in law and has an extensive teaching and research experience with different universities in Africa, Europe and the US.

SOUTH AFRICA

Gabriella Razzano is a senior fellow with RIA and legal consultant on issues of transparency, open data, technology and law. She holds a BA LLB from the University of Cape Town, and graduated with distinction in sociology. She clerked with Justice Yacoob of the Constitutional Court, and has also worked with the University of Witwatersrand, as well as with domestic and international non-governmental partners. She has contributed to the drafting of several regional instruments, such as the African Model Law on Access to Information and the African Declaration on Internet Rights and Freedoms. She is a Founding Director of OpenUP, an Internet Governance Fellow and an alumni of the International Visitor Leadership Program (Global Digital Leader). Gabriella is also the chairperson of the African Platform on Access to Information Working Group.

TANZANIA

Dr. Patricia Boshe is a co-founder and co-director of the African Law and Technology Institute (AFRILTI), a research institute focusing on the interrelation between law, technology and society from an interdisciplinary perspective. She is a Doctor of juris from the University of Passau, Germany, specialised in privacy and data protection. She also holds an LLM on IT and telecommunications law from the Open University of Tanzania. Some of her research activities involve an assessment and critique on the data protection legal reforms in Africa, including some focusing specifically on Tanzania, and on the digital divide and eAccessibility in Tanzania. Her publication record includes a book on data protection, book chapters and over a dozen international refereed journal articles, book reviews and practical legal comments.

UGANDA

Neema Iyer is an artist and a technologist. She is the founder and director of Pollicy, a civic technology organisation based in Kampala, Uganda. Pollicy uses data, design and technology to improve how citizens and government engage around public service delivery. She hold a Masters in Public Health from Emory University and has worked on large-scale mobile and digital projects across Africa as part of TTC Mobile (previously Text to Change) and Viamo (previously VOTO Mobile). She currently leads the design of a number of projects focused on building data skills, fostering conversations on data privacy and digital security, and innovating around policy. ■