REPORT ON ONLINE NARRATIVES ON DIGITAL ID IN AFRICA

Prepared by CIPIT

Strathmore University

Centre for Intellectual Property and Information Technology Law

CONTENTS

EXECUTIVE SUMMARY

BACKGROUND

The world, through the United Nations' (UN) Sustainable Development Goal (SDG) 16.9, has made a commitment to ensure universal identification (ID). It is estimated that around 1.5 billion people currently lack formal means of proving who they are, hindering their ability to among other things, access finance and vote. In recognition of the potential of digital technologies to foster inclusion, the World Bank Group (WBG) through its project, ID for Development (ID4D), has been supporting governmental efforts to set up and roll out Digital ID (DID) systems. While lauded as highly effective and accurate, the use of digital technologies in ID brings about a new set of concerns such as the violation of user privacy or discrimination on the basis of disclosed personal data. Aside from this, the cost of establishing DID systems is often high. Despite this, governments in Africa – and a number of private entities – have increasingly been turning to DID as a panacea to various developmental inadequacies.

PROBLEM

In the deployment of these programs, deploying authorities appear to lack concrete risk assessment tools that guide them. The Omidyar Network's (ON) GoodID principles identify aspirational, high level, standards of DID such as privacy, security, inclusion, user control and user value. The Centre for Internet & Society (CIS) has developed a range of tests to appraise an ID program such as the risks-based test which cautions deploying authorities to look out for risks such as data breaches. However, both the GoodID principles, and the CIS' risk-based test, are highly abstract in nature, limiting their ability to properly guide deploying authorities in determining when it is appropriate and proportionate to roll out a DID program. This shortcoming is understandable due to the relative novelty of DID systems in a number developing countries.

CONTRIBUTION

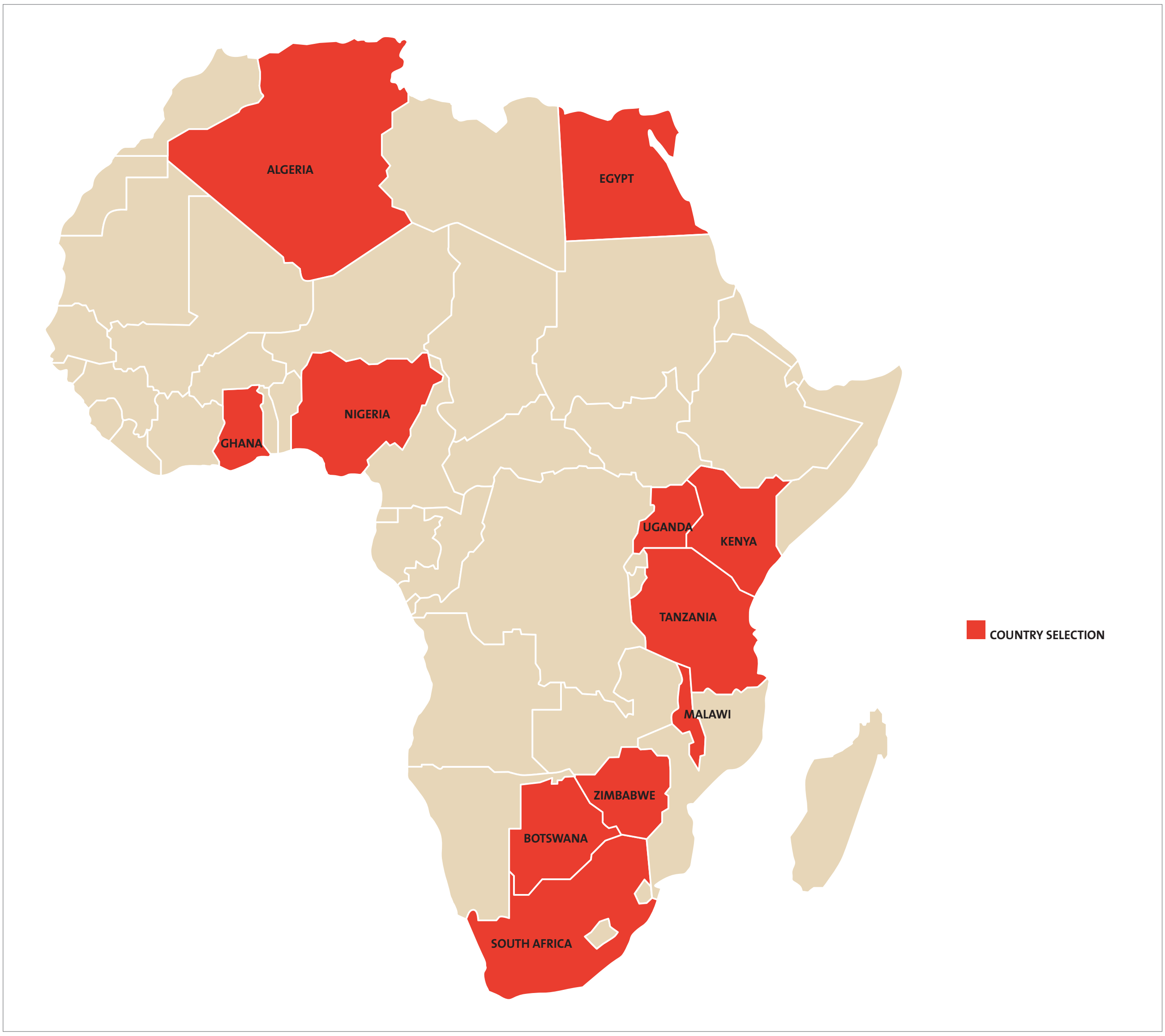
Increasingly, with the introduction of DID programs in a number of African countries, citizens and residents have taken to social media to elaborate on some of their experiences of ID and interacting with ID systems. Albeit limited in scope and magnitude, these online reports of lived experiences provide a useful tool for assessing the impact of DID and identifying likely harms to which users may be exposed. Analysing social media narratives from 11 African countries, this report identifies, in descending order of gravity, three major categories of harms affecting users, as well as instances when the harms are most likely to manifest.

Category One Harms: These harms are primarily associated with an inability to access foundational forms of ID. In countries where foundational ID (usually national ID) is equated with citizenship, those unable to access the ID are effectively locked out of the country's formal life. In the implementation of DID programs, this report finds that these harms are likely to manifest where there is a mass registration exercise that is highly centralised, mandatory and time bound. These exercises often fail to recognise persisting systemic exclusion, and in fact furthers such exclusions by entrenching corruption and bureaucratic practices, or by entrenching pre-existing identity-based biases. This category of harms is the gravest due to the extreme impact it has on people's lives. When confronted with the potential of this harm, deploying authorities ought to reconsider the entirety of the program.

Category Two Harms: Users can also face harms as a result of having access to ID. Harms in this second category relate to ID and its impact on constitutional rights, namely, the right to equality, privacy, and other human rights such as healthcare. The harms in this category include privacy violations such as fraudulent financial activity, and discriminatory practices such as denial of services on the basis of data disclosed in the application for an ID. These harms are most likely to occur where; there is an absence of data protection legislation, inadequate oversight and redress mechanisms, and an undefined scope of use for collected data. It is particularly exacerbated where the sector in which the ID is issued is a sensitive one such as finance or healthcare. These harms, according to this report, call upon deploying authorities to put a pause on the implementation and ensure that there exists a conducive environment for the widespread collection and use of data.

Category Three Harms: Unlike the first two, harms in this category are predominantly logistical/operational in nature. Essentially, these harms are the inconveniences faced by users in using ID, such as long lines, clerical errors, cumbersome processes etc. They may, in some instances, amount to grave violations of human rights (Category Two), but often can be remedied through sound project planning. These harms are likely to manifest where the target population is large and widespread, there is a lack of sufficient resources, and the rollout plan is highly centralised.

This report proposes the use of these categorisations in the assessment of DID programs.



ABBREVIATIONS

ABIS	Automated Biometric Identification System
BVN	Bank Verification Number
CHIFA	eHealth Care cards
CIS	Centre for Internet & Society
CNIBE	Carte Nationale d'Idetité Biométrique Electronique
DHA	Department of Home Affairs
DID	Digital Identification
EAC	East African Community
EBRS	Electronic Birth Registration System
GPMC	General Multipurpose Card
ID	Identification
ID4D	Identification for Development
IPRS	Integrated Population Registration System
KRA	Kenya Revenue Authority
KYC	Know Your Customer
NHIC	National Health Insurance Card
NHIF	National Health Insurance Fund
NIIMS	National Integrated Identity Management System
NIMC	National Identity Management Commission
NIN	National Identity Number
NRB	National Registration Bureau
ON	Omidyar Network
SDG	Sustainable Development Goals
UBR	Universal Beneficiary Register
UN	United Nations
WBG	World Bank Group

I. INTRODUCTION

a. BACKGROUND

The ability to identify oneself is often taken for granted. However, when one considers the number of interactions that require proof of identification (ID), the importance of any identifying documentation suddenly becomes apparent, be they government issued ID cards, passports, voter's cards, social security numbers and tax IDs, or privately issued login credentials for online banking. According to the World Bank, about 1.5 billion people are considered unidentified in the sense that they lack formal means of proving who they are, with most in Asia and Africa.[1] This in turn, affects their ability to vote, and to access healthcare, financial services, education, and social welfare.[2]

While a number of affected countries – which are in Asia and Africa – currently leverage traditional ID systems which are often paper based, advancements in technical capabilities have led the World Bank Group (WBG) to believe that modern technologies such as mobile devices, can be utilised to close the ID gap and facilitate wide-scale ID.[3] Consequently, the WBG embarked on the ID for Development Program (ID4D) to aid governments with funding in order to encourage and facilitate the use of Digital ID (DID).[4] This ambition is in line with the United Nations' (UN) sustainable development goal 16.9, which aims at ensuring all have ID by 2030.[5]

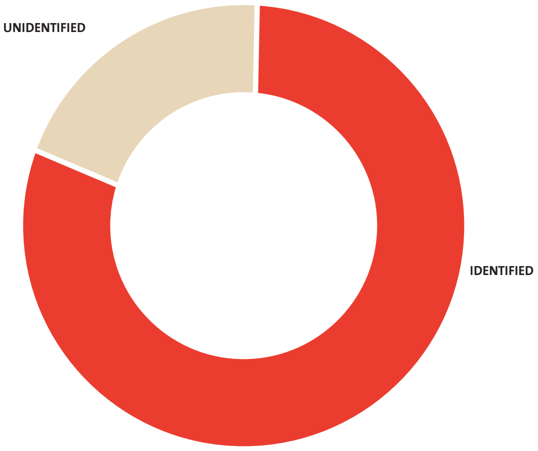


Fig. approximately 1.5 billion people lack formal ID

DID simply refers to the same identifying information one would use to register for paper-based systems – name, date of birth, place of birth etc. – but captured and stored digitally and often used in electronic transactions.[6] The two primary forms of data collected in DID registration are categorised as:

i) biographic, including name, gender and address; and
ii) biometric, including fingerprints and iris scans.[7]

Digital ID programs can generally be classed into foundational and functional.[8] The former refers to ID that serves multiple purposes, such as a country's national ID, while the latter refers to ID intended to enable access to a particular service, for example a health care insurance card or even a social media credential.[9] Perhaps the most notable foundational DID program in recent years is India's Aadhaar system.[10] In less than a decade, nearly the entire population was registered and made use of their unique Aadhaar ID number to, among other things, access government services, receive welfare disbursements and access private services such as those of financial institutions.[11] Functional systems have also mushroomed in a number of countries due to donor funding among other things.[12]

Inasmuch as these systems unlock a society's economic potential, improve service delivery and facilitate inclusion, there are salient risks that exist.[13] The example of Aadhaar is highly illustrative.[14] While extremely convenient at a margin of the cost of its rivals,[15] Aadhaar faces a significant amount of problems chief among them being cyber security concerns.[16] The constitutionality of the entire system was challenged at India's Supreme Court resulting in the revocation of a number of sections of the system's enabling legislation, the Aadhaar Act, for reasons including inadequate data protection mechanisms.[17] However, the system itself was largely upheld as constitutional.[18] Kenya recently attempted to roll out a centralised foundational DID program, the National Integrated Identity Management System (NIIMS), colloquially termed 'Huduma Namba'. The constitutionality of this system was challenged at the High Court of Kenya on somewhat similar grounds as in India i.e., privacy violations, potential mission creep and discrimination.[19] Much like in India, Kenya's Huduma Namba was also largely upheld as constitutional by the High Court.[20] It appears from these two cases – and from the adoption of DID programs in Nigeria,[21] and Ghana[22] – that DID programs are here to stay.

DID systems are often expensive to establish and run.[23] While the potential benefit to the population may sometimes make this investment seem appealing, the existing risks beg for some refrain in taking up these potential white elephants.[24] A good DID system may help realise all the ambitions discussed above such as financial inclusion and improved service delivery.

On the other hand, there equally exists the risk that the design or implementation of such programs may entrench existing barriers to equality, further discrimination and also open up the door to surveillance by the state or even private entities.[25] Therefore, sound planning for the implementation of any DID program ought to consider what harms users would be exposed to.

b. CONTRIBUTION

This report proposes a risk categorisation system to supplement the already existing factors that are considered when various entities – both public and private – seek to launch DID programs or issue ID in different contexts. Based on a small-scale collation of social media narratives spanning 11 African countries, this report elaborates on the risks associated with different forms of DID by highlighting the lived experiences of users of these programs. These experiences form the basis of the report's risk categorisation system which aims to be instructive for feasibility and performance studies into future and existing DID systems. This report is guided by two main frameworks discussed below, the Principles for Evaluation set out by the Centre for Internet & Society (CIS)[26] and the Omidyar Network's Good ID principles.[27]

[1] World Bank Group, Identification for Development (ID4D): Making Everyone Count, February 2016, -< http://pubdocs.worldbank.org/en/332831455818663406/WorldBank-Brochure-ID4D-021616.pdf accessed 15 May 2020.

[2] World Bank Group, Identification for Development (ID4D): Making Everyone Count.

[3] World Bank Group, Identification for Development (ID4D): Making Everyone Count.

[4] World Bank Group, Identification for Development (ID4D): Making Everyone Count.

[5] Sustainable Development Solutions Network, Indicators and Monitoring Framework, -< https://indicators.report/targets/16-9/ accessed 15 May 2020.

[6] GSMA, World Bank Group, and Secure Identity, Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, Discussion Paper, 11 -< http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf accessed 15 May 2020.

[7] GSMA, World Bank Group, and Secure Identity, Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, Discussion Paper, 11.

[8] Alan Gelb, and Anna Metz, Identification Revolution: Can Digital ID Be Harnessed for Development? Centre for Global Development, Washington DC, 2018, 2.

[9] Alan Gelb, and Anna Metz, Identification Revolution: Can Digital ID Be Harnessed for Development? 2.

[10] https://uidai.gov.in accessed 15 May 2020.

[11] Alan Gelb, and Anna Metz, Identification Revolution: Can Digital ID Be Harnessed for Development? 1-2.

[12] Gelb A, and Metz A, Identification Revolution: Can Digital ID Be Harnessed for Development? 2.

[13] Pam Dixon, 'A Failure to "Do No Harm" – India's Aadhar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.', 7 Health Technology, 2017, 540.

[14] Pam Dixon, 'A Failure to "Do No Harm" – India's Aadhar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.', 540.

[15] Alan Gelb, and Anna Metz, Identification Revolution: Can Digital ID Be Harnessed for Development? 2.

[16] Jain M, 'The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment', -< https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/ accessed 15 May 2020. See also, Khera R, 'Aadhar Failures: A Tragedy of Errors', 54(14) Economic and Political Weekly, April 2019 -< https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare accessed 15 May 2020.

[17] KS Puttaswamy and another v Union of India and others, 2018 (Supreme Court of India). For a discussion on the inadequacies of the system, see, Pam Dixon, 'A Failure to "Do No Harm" – India's Aadhar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.'.

[18] KS Puttaswamy and another v Union of India and others, 2018 (Supreme Court of India).

[19] Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR.

[20] Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR.

[21] https://www.nimc.gov.ng/the-e-id-card/ accessed 15 May 2020.

[22] https://nia.gov.gh/eidcard.html accessed 15 May 2020.

[23] World Bank Group, Digital Identity Toolkit: A Guide for Stakeholders in Africa, June 2014, viii, -< https://www.id4africa.com/articles/DigitalIDToolkitforAfrica2014EN.pdf accessed 15 May 2020.

[24] Pam Dixon, 'A Failure to "Do No Harm" – India's Aadhar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.', 540.

[25] Alan Gelb, and Anna Metz, Identification Revolution: Can Digital ID Be Harnessed for Development? 3. See also, Mahajan D, Sperling O, and White O, 'Digital ID: The opportunities and the risks', 19 August 2019, McKinsey Insights -< https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks accessed 15 May 2020.

[26] The Centre for Internet & Society, Governing ID: Principles for Evaluation-< https://cis-india.org/internet-governance/governing-id-principles-for-evalution accessed 15 May 2020.

[27] Omidyar Network, Omidyar Network Unpacks Good ID, May 2019, https://www.omidyar.com/sites/default/files/ON%20Unpacks%20Good%20ID_Final_3.7.19.pdf on 10 June 2020.

II. FRAMEWORKS

a. CIS PRINCIPLES FOR EVALUATION

The Centre for Internet & Society (CIS) has suggested a number of tests to evaluate DID programs.[28] These include rule of law tests, rights-based tests and risks-based tests.[29] Of these, the risks-based tests are the most relevant to this report's aims. The risks-based tests recognise the inherent challenges posed by DID programs as discussed above and propose the adoption of risk assessments by government preceding deployment.[30] However, with most DID systems being novel in African countries, there is little to go by in the way of conceptualising what harms are. It is possible to discuss abstract concepts such as privacy, surveillance and exclusion, but at such a high level, it would be difficult to assign weight to the potential harm and measure it up against the overall goals of a system, rendering the risks-based test somewhat useless. Over the past few years, a number of African countries have rolled out both functional and foundational DID programs or digitised existing ID systems. In addition to these, private institutions such as telecommunications service and financial service providers have digitised their offerings, issuing digital credentials to enable access. Both the public and private sector issued ID have been met with mixed reactions. Some of these reactions have manifested through users sharing their experiences over social media. Through an analysis of social media posts by users detailing their experiences with these programs, this report attempts to categorise the common harms faced by users. In doing so, this report provides an account of some of these lived experiences and extrapolates common themes therefrom. The identified categories are ranked in order of harm for purposes of conducting the risk assessments, making the endeavour more practical.

b. OMIDYAR'S GOOD ID PRINCIPLES

Recognising the substantial risks that DID programs pose viz, privacy violations, exclusion, surveillance and discrimination, the Omidyar Network identifies characteristics that DID ought to adhere to in order to qualify as 'Good ID'.[31] These characteristics are two pronged. The first is the practice or conduct of actors within the field of DID, their transparency, accountability and trustworthiness.[32] This practice cuts across all stages of DID, from the conceptualisation process to the eventual implementation. The putting in place of DID, especially by States – from this perspective – is thought of as a trust building exercise. The second prong sets out the design features important in DID programs:[33]

i) Privacy: practices that limit the exposure of personal data to unauthorised persons, adequate privacy safeguards baked into the system and due process mechanisms in place for instances of violations.

ii) Inclusion: minimal barriers to access, safeguards against discrimination on the basis of ethnicity, race, gender or religion, and mechanisms to rectify clerical errors that may result in exclusion.

iii) User Value: providing users with access, convenience, interoperability. The benefits must outweigh the risks users are exposed to in order to be valuable.

iv) User Control: transparency in the use of data, consent-based transactions, permissible user discretion in handling data, and administrative redress mechanisms in instances of violations.

v) Security: data integrity, cyber security, safeguards against human interference such as through corruption, and accountability measures in place.

The CIS proposed risks-based test advocates for risk assessments to be conducted prior to the deployment of DID programs. The risks that would be looked out for in such an assessment are precisely those identified in the Good ID framework by Omidyar; discrimination, surveillance etc. However, the CIS framework is useful only to the extent that the risk assessment instructs actors to look out for risks; it does not fully elaborate upon the nature of these risks nor does it set out the weighting of one risk vis a vis another. The Good ID framework provides some clarity in this regard by clearly enumerating how harm may manifest and conveniently labels them. Despite this, it also does not specify any value attachments to the harms for purposes of weighting.

Using these two frameworks, this report advances efforts to appraise the potential risks of DID programs by using lived experiences reported on social media platforms across 11 countries in Africa regarding various forms of ID. This report identifies the common harms reported in each country that has been studied and infers broader categorisations of harms that would guide risk assessments. These identified categories are ranked in order of level of harm.

[28] The Centre for Internet & Society, Governing ID: Principles for Evaluation, 23.

[29] The Centre for Internet & Society, Governing ID: Principles for Evaluation.

[30] The Centre for Internet & Society, Governing ID: Principles for Evaluation.

[31] Omidyar Network, Omidyar Network Unpacks Good ID, 2.

[32] Omidyar Network, Omidyar Network Unpacks Good ID, 2.

[33] Omidyar Network, Omidyar Network Unpacks Good ID, 3-6.

III. METHODOLOGY

a. SCOPE

This report analyses data gathered from social media posts. The collated data spans the following countries: Algeria, Botswana, Egypt, Ghana, Kenya, Malawi, Nigeria, Senegal, South Africa, Tanzania, Uganda and Zimbabwe. A total of 325 posts were collected. The selection of countries for this report was based on:

i) a country's recent introduction of, or migration to, DID;

ii) the cross section of data available from a particular country's users on social media (in essence, how many different users took to social media to describe harms); and

iii) the variety of DID (both private and public) being used in the country. We also attempted to cover the four major regions of the continent (North Africa, Eastern and Central Africa, West Africa and Southern Africa).

This information was collected from Twitter, Facebook, and, where referred to by social media users, a few online news sites. User posts which we gathered related to: National IDs, Passports, Driver's Licenses, National Health Insurance, Social Security, Refugee Cards, Tax IDs, banking credentials, and phone numbers. However, this is a non-exhaustive list. Naturally, each country's experience is radically unique, influenced by socio-political contexts. Therefore, the data is not uniform and, in some instances, some types of ID – usually government issued – features more than others. Once gathered, the harms in these social media narratives were categorised according to the Good ID principles that were violated by the respective authorities. This enabled the report to identify and develop the broader categorisation of harms.

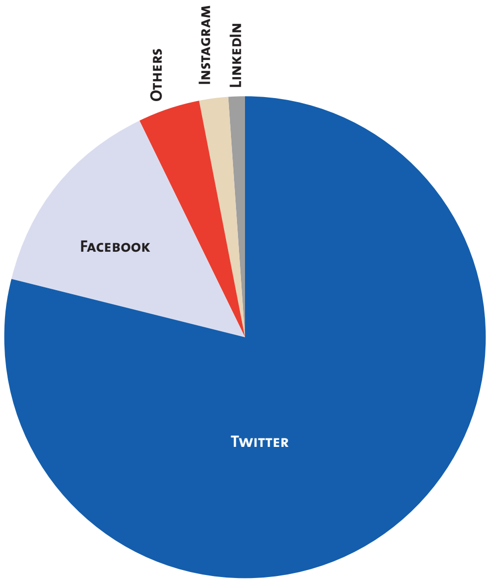


Fig. Sources of Narratives

b. LIMITATIONS

By nature of its design, this research possesses certain limitations. In particular, the chosen methodology suffers from selection bias in a variety of ways, such as those discussed below.

a. Due to the quantity available, the collated data is not representative.

b. A number of posts were authored in other languages, or used slang/vernacular, hindering search capabilities. Further, search parameters relied on key words associated with the country and the (D)ID in question; posts that excluded these words may not have been captured. Further, the research design herein essentially excludes persons without access to smartphones and by extension, social media.

Notwithstanding the limitations, this research provides numerous benefits for a variety of stakeholders. First, the report does not purport to definitively identify, and then generalise, the harms facing a particular country. Instead, its aim is to give a partially qualitative elucidation of the nature of the harms actually faced on the ground with a view to developing categorisations of these harms into risk levels.

This is 'partially qualitative' in that the explanation of harms users face will serve to paint a picture of the practice on the ground, while the statistical representations will serve to indicate the scale of the problem. The categorisations developed will then serve to guide risk assessments. For example, if fraud is identified as persistent and the complaints relating to fraudulent activity predominantly relate to implementation/operationalisation, this would be highlighted within the categorisations and the recommendations. Second, the minimal data gathered through these platforms is construed, in this report, as indicative of the situation in the country thereby obviating concerns arising from the limited nature of the collation.

IV. CATEGORISATIONS

In the appendix to this report, user accounts of experiences with government and privately issued ID are discussed in moderate detail. Each country discussed presents its own unique challenges. However, from the narratives, certain characterisations of the nature of harms faced by users can be made. These fall on a spectrum and would require different reactions or mechanisms to address them. In this section, the report identifies these broader categories of harm discernible from the discussion of findings in the appendix. These categories serve two primary functions: to paint a picture of the current state of harms related to DID faced in these regions, and to allow governments and private entities weigh the risks of these harms against the objectives sought. In developing these categories, caution was exercised to ensure generalisations were not made from insufficiently representative data. Therefore, the categorisations below do not serve to conclusively explain the predominant forms of harm in any of the countries or regions. Rather, based on user accounts, they typify harm based on the gravity and magnitude.

As stated in the introduction of this report, deploying DID calls for a balance to be struck between the intended benefits of identifying the population and the inherent risks associated with DID. Some risks are such that it would not be worth it to embark on a project. Others are relatively easier to address either during or after the rollout. The main limitation faced in making these categorisations is positing the utility that would be derived. A major objective of this report has been to elaborate upon the CIS proposed risk-based tests by typifying the harm described therein; to move from the abstract to the concrete. However, these categorisations are based on events that have already passed or are currently in progress, therefore it would appear that they are more of a situational analysis than a pre-emptive tool. To address this, the report describes these harms in a neutral manner, facilitating their applicability to future projects and risk assessments. The practical utility of this would be to indicate the spectrum of negative outcomes one may expect. The closer one is to the first category (the most harmful), the less feasible a project is. Establishing whether a project is likely to fall within a category is a highly contextual endeavour. The report therefore proposes a few factors that may contribute to the fruition of the feared risks in order to equip respective project managers/government officials with an idea of what to look out for. The categories are discussed below.

a. CATEGORY ONE HARMS

In nearly all the countries reviewed, the most complained of harm regarded access to ID in general. These constituted violations of the inclusion and user control principles of Good ID. A common theme in a number of countries was an ID ecosystem that was structured in a manner that systemically perpetuated exclusion, and consistently locked people out of formal systems. The trend appears to be guided by the following arc: a country adopts a policy equating the national ID to citizenship, the country rolls out mass registration with crude incentives such as expiry dates and impending denial of service, the rollout is marked by significant corruption that results in the exclusion of large sections of the population, and finally, the excluded people are unable to access basic services or obtain other legal documentation that would serve to identify them due to lacking the initial breeder document.

The harms in this category are attributable to the inherent nature of the ID in question (often foundational) and the manner in which it is operationalised. Due to the importance of foundational documents, lacking access immediately excludes users from the formal life of the country. The clear and immediate source of the harm associated with foundational documents lies in their equation to citizenship. This should not be the case bearing in mind the systemic barriers that exist to accessing it. The research revealed a number of users who have lived in their respective countries all their lives but have been unable to obtain the foundational ID in use. Whereas the approximate number of unidentified people in a population is largely known, their experiences resulting from being unidentified remain inconclusively considered by existing research. From the research conducted, this report noted that the common experiences of such people have been, among other things, preclusion from job opportunities, mobility and access to finance. The WBG ID4D aims to increase identification through facilitating the use of DID. Merely introducing a foundational DID does not serve to address this goal. This is more so the case where it is equated to citizenship without addressing the pre-existing structures that serve to disadvantage sections of the population that have historically been excluded. With regard to the operationalisation of these systems, an absence of sound project management often results in logistical nightmares and gives way to corruption at the lower levels. With potential backlog, considerable autonomy in the hands of registration officers and a policy advocating a punitive approach to those who fail to obtain the DID, users become subject to solicitations for bribes in order to make the process easier. These serve to exclude those unable to afford these bribes or are unwilling to pay.

The data analysed indicated that users who were unable to access national ID were further precluded from obtaining other forms of ID. On the extreme end of the impacts arising from this reality was users being unable to secure formal employment for years on end. Slightly less drastic, while nonetheless problematic, were accounts by users who were unable to obtain time-bound ID such as e-Passports which were often rolled out on a strict schedule. Both these impacts however, stem from the same harm – an absence of access to ID.

This category would primarily relate to government issued ID. Predominantly, national IDs would feature, however, even other documents such as Passports and Birth Certificates may very well fall into this category. These harms should be anticipated where:

i. A country is introducing a novel foundational DID system through mass registration without any allowances for a phased approach and clear communication regarding the potential for concurrent use of the pre-existing ID or alternatives;

ii. A country's proposed DID is equated to citizenship and the method of implementation is more coercive than it is encouraging of use. DID projects should be beneficial to users and enrolment should be on the basis of the perceived benefits one would obtain and the ease of the process; or

iii. A country's registration process is heavily bureaucratic and vests significant authority in civil servants without any due process framework to hold them accountable. ID registration should not be framed as a benefit one obtains at the mercy of a registration official. This leaves room for bribery and corruption.

The above instances are by no means conclusive. However, from the data analysis, these are some of the factors that contribute to the harm in this category.

b. CATEGORY TWO HARMS

This second category of harms is partially similar to the first. Harms in this category are those inherently linked to fundamental constitutional rights such as those of privacy, equality, and third generation human rights such as that to health. While exclusion – identified in the first category – often means that one would be unable to realise these rights (for example of ownership over property), there are other harms users experience despite (or as a result of) having the ID in question. This category deals with those harms that users face due to an improperly implemented DID system; when the harms they are exposed to are from having the ID rather than from being excluded. From the narratives, this category of harms was particularly prevalent where there existed inadequate privacy safeguards in place. These harms were not exclusive to government issued ID. Examples of these harms include the collection of highly sensitive personal data without any frameworks in place to prevent mission creep. From national IDs requiring information pertaining to religious beliefs to banks requiring an overwhelming amount of information in the name of Know Your Customer (KYC), users were exposed to the negative effects of issuing authorities possessing a large amount of data about them. It was not uncommon for users to complain of fraudulent activity for example in relation to their bank accounts or mobile money wallets. The abundance of personal information collected coupled with inadequate limitations such as purpose driven constraints, users found themselves on the receiving end of unsolicited marketing messages, fraudulent financial transactions and on the more extreme end of the spectrum, discrimination on the basis of that personal information. These harms are compounded where the databases are interoperable, and access is not regulated. Another harm in this category is government surveillance resulting from highly centralised and extensive collection of personal data.

In the countries reviewed, the most common manifestation of this harm was perhaps fraudulent activity linked to privacy violations. Users complained of fraud linked to their credentials issued by financial institutions, and identity theft linked to their government issued IDs. Furthermore, some users complained of transacting with businesses which required a significant amount of their personal details and thereafter received unsolicited marketing messages. In rarer but highly harmful cases, users gave accounts of discrimination they were subjected based on the amount of personal data disclosed.

Based on the narratives, this category of harms is most likely to occur in instances where:

i. Data protection legislation is non-existent or ineffective;

ii. The practice of administering DID programs does not adhere to core data privacy principles such as purpose and time limitations;

iii. The collection of data by private entities is not regulated or overseen by a responsible authority;

iv. The scope of data collected for basic purposes is too wide; or

v. The country in question, or the relevant sector the DID is being deployed in, is naturally prone to violations of privacy or perpetuation of fraud (such as health and finance).

Avoiding this category of harms largely depends on the putting in place of sound data protection frameworks that prioritise users' fundamental rights. This category of harms is much akin to the CIS proposed rights-based tests which focused on the impact of DID systems on user rights. This report finds that these harms do not rise to the level of category one harms but are nonetheless crucial enough to call for a pause in roll out where any of the particular conditions that are conducive for the harms to take place exist. In particular, they call upon deployment authorities to review if the objectives sought can be achieved in a different manner.

c. CATEGORY THREE HARMS

Unlike the first two categories which pose significant risks to the wellbeing of citizens, harms in this category are comparably moderate. Nonetheless, in some instances, these harms may graduate and end up in either of the first two categories. Harms in this category primarily have to do with the logistical implementation of ID systems at a large scale. The Good ID principles often violated with harms of these nature are User Value and User Control. From the narratives, it was noted that poor project management often resulted in minor inconveniences such as clerical errors in a user's particulars or considerably long wait times. While on the face of it these are minor inconveniences (as compared to widespread privacy violations), they may indeed be exacerbated in some instances. For example, in Nigeria, users complained of delays to the tune of over a year; a delay that denies applicants access to many life opportunities. However, on the whole, the harms faced in this category often do not adversely affect users' rights with the exception of amounting to a nuisance frustrating their daily use. This research found harms such as security measures (often in the financial sector) that are too burdensome and end up locking out the actual user. It also found a widespread inability of users to rectify or update their details easily, having to comply with tedious processes administered by customer service representatives or government officials. This absence of control makes it cumbersome to use ID. Perhaps most importantly was the use of the ID in question and its limitations. Often, users would complain of being overidentified and not deriving a 'one-stop shop' value from core documents.

Other frustrations users highlighted included rude customer care representatives/government officials and unpredictable wait times.

The research noted that harms in this category often take place where:

i. The target population is large and spread out;

ii. There aren't sufficient resources (both technical and human) to meet the demands of roll out;

iii. There isn't any verification mechanism to ensure error rectification and deduplication takes place; or

iv. The roll out plan is not decentralised, and users have inadequate information regarding requirements.

In this category issuing authorities ought to primarily take care that the trivial issues of implementation do not compound and amount to the violation of rights or exclusion of persons altogether. This of course is highly dependent on the ID in question. For more sensitive forms such as financial ID, more care is urged. However, the potential for these harms existing, is not by itself, a disqualifying factor. Issuing authorities can address this by employing sound project management strategies.

V. OUTLINE OF HARMS BY COUNTRY

COUNTRY	HARMS DEDUCED FROM FINDINGS	GENERAL COMMENT
Algeria	While Algeria has digitised many of the nationally issued forms of ID (passports, national ID, driver's licenses etc.), the bulk of user posts related to the passport. In particular, Category Three Harms were the predominant form, with clerical errors on passports. However, there were a number of Category Two Harms in relation to dual citizens.	Data collection was severely limited by language barriers. An absence of user control was noted from the fear users had regarding errors in the process.
Botswana	The bulk of posting by users in Botswana detailed their experiences with the national ID/'Omang Card'. Users highlighted Category One Harms that arose from the barriers to obtaining an Omang card, and the government's equating the card to citizenship. This was, to a lesser extent, also the case with passports. On the whole, the harms experienced by users in Botswana related almost exclusively to access. However, there were a few instances of Category Two Harms with users pointing out instances of unsolicited marketing messages from vendors they hadn't interacted with.	Search findings were moderately hindered by language barriers. Access concerns were predominant in posts.
Egypt	Harms reported in Egypt appeared to be a meld of Category One and Two Harms. With tensions between religious groups in the country, users noted that the requirement to disclose one's religious belief opened up room for discrimination in issuance of ID and later, in exercising rights such as voting. Aside from perpetuating exclusion, the expansive collection of data also facilitated infringement of constitutional rights.	Data collection was severely limited by language barriers. However, the main issue related to access.
Ghana	In relation to Ghana's national ID, the Ghanacard, users elaborated on harms that would fall under the first category – relating to access. The Ghanacard is equated to citizenship by the State and access is hindered by a number of barriers including corruption in the process. An inability to access this card prevents citizens from accessing further documents such as passports. Users also raised concerns about the passports, and the entrenchment of illegal processing payments that hindered their access.	The main concern in Ghana was accessing a national ID that is crucial for public life.
Kenya	User posts in Kenya relating to the national ID exhibited the existence of all categories of harms. From exclusion that is compounded by the equation of the ID card to citizenship, to the bureaucracies associated with applying for the ID, to the violation of privacy associated with telcos that handle customer data, particularly ID. Similarly, users applying for passports indicated that unnecessary delays and bureaucracies plagued the process. The introduction of a centralised DID, the Huduma Namba, also led to confusion regarding the status of the existing ID and raised concerns around the expansive nature of data collected.	Data collected from Kenya was significantly higher than other countries. The recorded harms span all categories, with an alarming number falling within the first two categories.
Malawi	In relation to the national ID, users complained of deadlines and insufficient information regarding the mass registration the country conducted. This affected accessibility. However, there were also positive indications that the mass registration was relatively successful. Users applying for driving licenses did note that corruption hindered their access.	Despite deploying varied search parameters, stringing together different key words, not much data was gathered from Malawi. However, the little gathered was indicative of certain trends.

Nigeria	Nearly the entirety of the gathered data details user experience with Nigeria's National ID. In particular, their inability to obtain one. Delays spanning years were not uncommon, and the application process was reported as being marked by corruption. Relatedly, users faced Category Three Harms with long queues and clerical errors in their documentation. This was also the case when it came to passports and driver's licenses. Users also faced harms in the second category. Some users complained of registration officials accessing their unique Bank Verification Number to ascertain their liquidity, and using that information to determine the illegal payment one would have to make in order to get an ID. A clear violation of their privacy.	Perhaps due to its population, Nigeria yielded the highest number of user posts. These were predominantly Category One Harms.
South Africa	User posts from South Africa largely gave accounts of minor third category harms – delays, long queues, and clerical errors.	South Africa's ID system was comparably unproblematic.
Tanzania	In Tanzania, the roll out of ID system was tied to the registration of SIM Cards. Whereas the process of applying was marked by delays and an inconsistent procedure across the country, users had to contend with the reality that their SIM cards would be disconnected if they were unregistered. The bulk of the user narratives all point to poor project planning/ implementation.	The harms faced by users were largely as a result of poor project planning.
Uganda	In Uganda, users largely complained of Category Three Harms – delays and clerical issues. Fraud or systemic exclusion weren't very common.	Harms identified in the country were largely trivial when compared to graver harms such as exclusion and had more to do with the implementation.
Zimbabwe	Harms identified from user posts included high costs attached to passports, discrimination in the application process for the ID and a cumbersome process.	Not much data is available on Zimbabwe's ID ecosystem.

VI. CONCLUSION

DID programs are currently in vogue. Using buzzwords like 'financial inclusion' and 'widening the net of social welfare' – both of which are valid and noble goals – governments and private entities introduce DID in various aspects of life. However, from various experiences around the world such as India's, it is clear that risks do exist.

The existence of risks alone is not sufficient enough to justify abandonment of projects that have the potential to improve the lives of billions of people. Risk mitigation ought to be undertaken. With harms relating to DID programs often being abstract and conceptual, it is difficult for issuing authorities to quantify these harms. The findings of this report, based on lived experiences, serve as a proposal of how to move from abstract to concrete.

Through the three risk categories, this report hopes issuing authorities would be able to determine when DID programs are proportionate to the goals sought.

APPENDIX: FINDINGS IN INDIVIDUAL COUNTRIES

This section contains the findings of the report. It begins by discussing the state of digital ID in each country. In the research, it was noted that a considerable amount of DID is issued by the government, justifying the inclusion of these brief country profiles. The profiles do not serve to limit the scope of ID considered in this research; other forms of ID feature in the findings. After describing the country's ID ecosystem, the report then moves onto highlighting the general cross section of the data relating to each country before delving into some specific complaints by users which are indicative of a general theme in the country in question.

a. ALGERIA

The government of Algeria has, since 2012, been pursuing a policy of digitisation of government services. The culmination of this push is the issuance of biometric national IDs termed Carte Nationale d'Idetité Biométrique Electronique (CNIBE).[34] Prior to this, the country migrated to ePassports.[35] Additionally, the same provider of the ePassport and CNIBE also worked on the country's eHealth Care cards (CHIFA).[36] The country utilises a single National Identity Number (NIN) for the ePassport and CNIBE to prevent errors and avoid duplication. In 2019, the country introduced a biometric points-based Driver's License. [37]

Available social media data primarily related to the National ID, Driver's License, Voter's Card, Passport and Refugee Card. 63% of identified posts related to the country's passport and larger immigration system. Citizens and residents took to Twitter to express a general fear among applicants of Algeria's ePassport that the issuing authorities would make clerical errors such in the spelling of applicants' names – evincing the absence of user control associated with the DID. Furthermore, the reports relating to the passport indicate that dual citizens are subjected to substandard treatment, being required to adhere to formalities prior to entry into Algeria such as visa application. Aside from this, there have been instances of journalists of Algerian citizenry being prohibited re-entry despite having valid Algerian passports in what appeared to have been some form of repression. A particularly alarming instance was the loss of a visa applicant's passport at an Algerian Embassy in Beijing by the embassy staff.

Posts relating to other forms of ID were relatively unproblematic. However, two users highlighted the existence of corruption in the application process for Voter's Cards and Driver's Licenses.

There were no recorded instances of privately issued ID raising any cause for complaints. However, data relating to Algeria was particularly scarce and data gathering was limited by language barriers due to a number of users sharing posts in Arabic and French.

b. BOTSWANA

Botswana's identification ecosystem has been identified as being relatively advanced in comparison to other Africa states.[38] Contributing to this is the country's ID life cycle which prevents a large number of people from falling through the cracks and ending up unidentified.[39] Without birth registration, ID registration cannot be issued – the potential for exclusion is clear in such a system. Citizens are issued a unique number at birth which is then used to obtain a national ID at the age of 16 years.[40] The ID, though not electronic, is machine-readable and barcoded with

[34] Stephen Mayhew, 'Algeria begins issuing biometric national identity cards this month' Biometric Update, 5 January 2016, -< https://www.biometricupdate.com/201601/algeria-begins-issuing-biometric-national-identity-cards-this-month accessed 9 July 2020.

[35] https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/new-national-identity-card-algeria accessed 9 July 2020.

[36] https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/new-national-identity-card-algeria accessed 9 July 2020.

[37] https://www.dzbreaking.com/2019/06/03/biometric-point-based-driving-license-issuance-generalized-countrywide/ accessed 9 July 2020.

[38] World Bank Group, The State of Identification Systems in Africa, 2017, 18 -< http://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf accessed 9 July 2020.

[39] World Bank Group, ID4D Country Diagnostic: Botswana, 2016, vi, -< http://documents1.worldbank.org/curated/en/864651486101539760/pdf/Botswana-ID4D-DiagnosticWeb040418.pdf accessed 9 July 2020.

[40] https://www.gov.bw/civil-registration/national-identity-card-application accessed 9 July 2020

biometrics. This ID is used to apply for other documents such the ePassport and driver's license i.e. it is a breeder document. This national ID is also referred to as the 'Omang Card'. In 2019, the Blue Card was introduced and caters to persons who have renounced Botswana citizenship, permitting them to live in, work in, and visit Botswana.[41]

Social media posts in Botswana related to the Omang Card, the Passport and the Blue Card. In relation to the Omang card, the majority of posts elaborate on the potential for exclusion that exists, namely, the cumbersome process of obtaining it and the difficulty accessing basic services without it – even private services such as from financial institutions. For example, without an Omang card, one cannot vote. At the same time, one particular post noted that non-citizens have been found with the Omang card, thereby attempting to justify the significant barriers to obtaining it.

Similar sentiments were expressed in posts relating to the Passport. Approximately 20% of identified users noted that the application process is cumbersome and filled with bureaucratic practices. The severity of the process is exacerbated for persons who recently renounced another country's citizenship.

In relation to user privacy, posts indicated that the practice of administering these ID programs fails to safeguard user information. 10% of identified posts highlighted receiving unsolicited text messages after sharing their particulars with vendors. Relatedly, the compulsory adducing of unique ID numbers for transactions with private businesses is also a cause for concern.

From the findings in Botswana, it was apparent that the main issues related to the Omang card. In particular, the significant barriers to access (both formal and informal) which perpetuates exclusion, and the equation of the Omang card to citizenship, thereby systematically disenfranchising an already excluded section of the population. The fact that this document serves as a breeder to other public and private documents means that not having it amounts to not having a formal life in the country.

c. EGYPT

Egypt's national ID is compulsory for all above the age of 16 years and is used to access a number of government and private services. While it is not electronic, in 2015, the Egyptian Government entered into an agreement with MasterCard to enable mobile money on the national ID card in order to facilitate payments of government charges for services.[42] Egypt's national ID has historically been wrought with discrimination concerns, particularly on the basis of religion.[43] The government also launched an electronic health insurance card in 2018.[44]

Identified posts in Egypt exclusively relate to the country's National ID. Approximately 30% of posts highlighted the potential for exclusion and discrimination that exists. Specifically, that the National ID requires a large cross-section of personal data that could be used for discrimination – an instance of voter suppression on the basis of religion was highlighted. Further, the cost of a National ID was noted to be higher for non-degree holders. Aside from these issues, there were privacy concerns – 11 % of posts alluded to unconsented information sharing. Lastly, a singular post highlighted the difficulty in applying for the National ID due to the queues.

Discrimination as a result of the invasive amount of data requested when applying seems to be the primary issue in Egypt. This isn't the only aspect perpetuating exclusion; the barriers to access such as differentiated cost also limit the number of people who can obtain a National ID.

Much like Algeria, Egypt also presented challenges in data gathering due to a large number of posts being in Arabic.

[41] http://www.xinhuanet.com/english/2019-08/22/c_138329546.htm accessed 9 July 2020

[42] ITU-T Focus Group on Digital Financial Services, Review of National Identity Programs, 2016, 19, 45 -< https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review%20of%20National%20Identity%20Programs.pdf accessed 9 July 2020.

[43] ITU-T Focus Group on Digital Financial Services, Review of National Identity Programs, 2016, 34.

[44] https://www.egypttoday.com/Article/1/45025/Egypt-launches-health-insurance-smart-card-system accessed 9 July 2020.

d. GHANA

Ghana recently introduced an electronic ID dubbed the 'Ghanacard'.[45] This multipurpose card, launched in 2018, is required to access bank accounts, passports, SIM cards, driver's licenses and other services. Both citizens and non-citizens residing in Ghana are eligible.[46] Ghana also issued a National Health Insurance Card (NHIC) which is biometric.[47]

Identified posts in Ghana relate to the Ghanacard and Passport. Of the posts relating to Ghana's Passport, both formalised and illegal processing payments were noted as entrenching exclusion. The former relates to an official express payment system available, while the latter, bribery. Users also complained of the passport's short duration of validity, hindering their continued use.

Complaints relating to the Ghanacard almost exclusively allude to the dangers associated with the categorisation of the ID as the sole proof of citizenship. To begin with, about 19% of posts highlighted the existing barriers to obtaining a Ghanacard such as requiring citizens to indicate their digital postcode yet not all citizens have smartphones. This harm is particularly exacerbated due to the fact that the Ghanacard, as a matter of government policy, is equated to citizenship. Despite this equation to citizenship, the government appeared not to have expedited the process for citizens to obtain this card. Reports exist of government officials in some localities capping the number of applicants at fifty per day despite the queues being much longer.

In relation to user privacy, one user commented that in response to some fraudulent practices, a major newspaper published images and personal data of Ghanacard holders. The post further called upon the Data Protection Commission to look into it. The primary issue in Ghana appears to be similar to Botswana and Egypt – a national ID highly central to daily life but hard to obtain for a large chunk of the population.

e. KENYA

Kenya's national ID has a long and problematic history, steeped in discrimination, exclusion and corruption.[48] With the introduction of the integrated population registration system (IPRS),[49] the national ID was digitised. Despite the existence of the national ID as a central ID, the Kenyan government introduced the National Integrated Identity Management System and issued a new unique ID number which it colloquially termed 'Huduma Namba'.[50]

Rather contradictorily, the government stated that this would be the single source of identity in Kenya. It is, ironically, supposed to exist alongside the national ID with the goal of eliminating duplication. Kenya also recently introduced the East African Community (EAC) e-Passport.[51] Other sources of digital identity in the country include the Kenya Revenue Authority (KRA) Tax PIN, National Health Insurance Fund (NHIF) card and the recently introducing digital driving licenses.

In Kenya, 38% of the gathered narratives related to the National ID, 28% to the Huduma Namba, and 10% to the passport. A negligible amount related to refugee cards, tax ID and drivers' licenses.

The existing historical problems plaguing the national ID were not addressed in the IPRS digitisation as can be gathered from the online narratives. Exclusion and corruption (which are sometimes related) appear to be the most salient issues. One post highlights the plight of a member of the Nubian community, a minority in Kenya, who lost his national ID and was unable to replace it for 30 years.

Another highlights illegal barriers put up by officers in charge of registration such as requiring school leaving certificates in order to apply for the ID. In other instances, police officers charge citizens for police abstracts which are needed for reporting a lost ID. Further, posts indicate the

[45] https://www.nia.gov.gh/ghanacard.html accessed 9 July 2020

[46] https://www.nia.gov.gh/ghanacard.html accessed 9 July 2020.

[47] http://www.nhis.gov.gh/bioid.aspx accessed 9 July 2020

[48] Kenya National Commission on Human Rights, An Identity Crisis? A Study on the Issuance of National Identity Cards in Kenya, 2007, -< http://www.knchr.org/Portals/0/EcosocReports/KNCHR%20Final%20IDs%20Report.pdf accessed 9 July 2020.

[49] https://www.immigration.go.ke/integrated-population-registration-systemiprs/ accessed 9 July 2020

[50] https://www.hudumanamba.go.ke accessed 9 July 2020.

[51] Cyrus Ombati, 'Deadline for new passport moved again by a year' The Standard, 25 February 2020, -< https://www.standardmedia.co.ke/article/2001361703/deadline-for-new-passport-moved-again-by-a-year accessed 10 July 2020.

extent of exclusion from other services that results from not having an ID – one user was unable to obtain a police clearance certificate due to not have a copy of his lost ID despite the fact that he lodged a replacement request.

Away from government, users noted a significant amount of fraud perpetrated in relation to private financial institutions such as banks and mobile money service providers. A few posts complained of the duplication of SIM card registration enabling criminals to take mobile money loans in other people's names simply by knowing their national ID number and name. This problem has escalated to the extent that the Communications Authority of Kenya has got involved.[52]

Narratives on Kenya's national ID also noted delays and barriers put up by bureaucracy leading to long wait times and uncertainty. It is prudent to note, in light of all this, that the government of Kenya treats the national ID as the single proof of citizenship (the Huduma Namba is yet to be fully implemented). Therefore, without it, as has been noted by some users, one cannot get formal employment, own property or conduct other legal transactions.

In both private and public sector, practices engendering privacy were lacking. A number of posts from state corporations such as the Kenya Power and Lighting Company and from private financial institutions required users to send copies of their IDs when requesting basic account related services. These practices existed long before Kenya enacted its Data Protection Act. Aside from the privacy implications, this indicates a low level of user control over the ID.

In relation to the Huduma Namba, a number of users queried the difference between the national ID and Huduma Namba, noting that everything the government alleged the latter would do, the former already did. This was of particular concern owing to the cost of the program and the invasive nature of the data collected. Some posts noted the absence of coordinated messaging from the government regarding serious considerations such as the use of the Huduma Namba to access government services. While registration was not compulsory (due to a court order), various government officials alluded to denial of service to persons who failed to register. In some alarming instances, government officials equated the Huduma Namba to citizenship. One user complained of being denied access to a National Health Insurance Fund Card due to lacking a Huduma Namba – this was during the period where the constitutionality of the entire program was in question before the High Court and there existed order barring the use coercion in registration. Another user rightly exhibited suspicion over the government's coercion of its own citizens while indicating the risks of centralising personal data to the stated extent without any privacy safeguards in place (at the time, Kenya's Data Protection Act was not in force). In a rather alarming complaint, one user detailed how a registration official accessed her personal details and harassed her. Similar exclusion and corruption related concerns that exist in relation to the national ID were highlighted by users in relation to the Huduma Namba. An important observation by some was the systemic exclusion that results from requiring a national ID in order to qualify for a Huduma Namba yet obtaining the former was already very difficult.

In relation to Kenya's passport, the online narratives stem from the country's switch to a new biometric East African Passport. Users have complained of inordinate delays that are unjustified, and a duplicative process that attempts to digitise some aspects but fails to eliminate manual processes that more or less make redundant the digitisation.

[52] Sam Okuoro, 'Communications Authority raises alarm over SIM cards scam', The Standard, -< https://www.standardmedia.co.ke/business/article/2001368948/communications-authority-raises-alarm-over-sim-cards-scam accessed 9 July 2020.

The core issues identified in Kenya's ID ecosystem include systemic exclusion, fraud, and inadequate service delivery in the operationalisation of ID systems. The inconsistent information regarding government issued ID (particularly the national ID and Huduma Namba) violate legitimate expectations and leave users in a state of limbo. Another issue that existed was the widespread violation of privacy as could be deduced from the SIM card duplication fraud and unsolicited marketing messages users complained of. However, the Data Protection Act came into force in late 2019 and is anticipated to address these concerns. \

f. MALAWI

The National Registration Bureau (NRB) issues national IDs to all Malawians aged 16 years and above. Prior to this, the country's voter's card was used as the primary form of ID.[53] The NRB implemented the Electronic Birth Registration System (EBRS) to enhance birth registrations.[54] The country is also embarking on a social welfare system referred to as the 'Universal Beneficiary Register' (UBR).[55] Malawi intends to, and is in the process of, linking all forms of ID to the national ID for ease of service delivery.[56]

Approximately half of the identified posts related to the country's national ID. The posts present a mixed bag with some commending the government for the speed with which the universal ID was issued and some expressing concerns around exclusion of the poor and marginalised by means of a deadline and fine for missing the said deadline. Additionally, some users queried for the application process both locally and abroad, indicating inadequate sensitisation on the process. In the recent election registration period (2019/20), some users complained of ineligible minors being issued IDs in order to enable them vote – an instance of election fraud. 38% of posts, which discussed the country's driving license, painted a largely negative picture. Users complained of corruption and delays. From this data, it appears that the core issue facing the ID ecosystem is the existence of fraud. There weren't any noted instances of privacy violations or an absence of user value. The existence of deadlines for the National ID contributed to exclusion as well.

g. NIGERIA

Nigeria recently made the switch to an electronic ID. The National Identity Management Commission (NIMC) issues Nigerians with a unique National ID Number (NIN) which is then used to issue an electronic ID in the form of a General Multipurpose Card (GMPC).[57] The uses include identification, payment (through a partnership with MasterCard [58]), travel and other yet to be activated services such as a health card functionality.[59] Persons above the age of 16 are required to obtain an e-ID. Nigeria also transitioned to an ePassport.[60] The country's Central Bank also issues a biometric Bank Verification Number (BVN) that serves as a universal ID across all commercial banks in the country.[61]

Of the total posts gathered for this entire report, Nigeria represented the bulk, with 23% of all identified posts. Half of these posts regarded the country's e-ID, just under 20% concerned the BVN, and driver's licenses accounted for approximately 18% of the posts. The remainder of the posts regarded the multiple forms of government issued ID in general.

Nearly all the posts by users in Nigeria paint a grim picture. In relation to the country's national ID, approximately 80% of users complained of delays in issuance. These delays were not minor – in some cases they were delays of about 8 years. Users complained of missed opportunities due to not having an ID card. Rather concerning is the fact that a number of users requested that the voter's card be used as a national ID due to the fact that it is easily issued, especially around election cycles. One user went as far to express concern that in seeking to populate the voter roll,

[53] GSMA, Digital Identity Country Report: Malawi, 2019, 7 -< https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf accessed 9 July 2020.

[54] GSMA, Digital Identity Country Report: Malawi, 2019, 5.

[55] GSMA, Digital Identity Country Report: Malawi, 2019, 11.

[56] UNDP, 'Moving towards a harmonized National Identity System in Malawi', 29 October 2018, -< https://www.mw.undp.org/content/malawi/en/home/presscenter/articles/2018/04/23/towards-a-harmonised-national-identity-system-in-malawi.html accessed 9 July 2020.

[57] https://www.nimc.gov.ng/the-e-id-card/ accessed 9 July 2020.

[58] MasterCard, MasterCard Government Services and Solutions Case Study: Nigeria National ID Card https://smartcitiescouncil.com/system/tdf/public_resources/Nigerian%20National%20ID%20card.pdf?file=1&type=node&id=2069&force= accessed 9 July 2020.

[59] https://www.nimc.gov.ng/the-e-id-card/ accessed 9 July 2020.

[60] https://immigration.gov.ng/enhanced-epassport/ accessed 9 July 2020.

[61] https://www.cbn.gov.ng/Out/2017/BPSD/Circular%20on%20the%20Regulatory%20Framework%20for%20BVN%20%20Watchlist%20for%20Nigerian%20Financial%20System.pdf accessed 9 July 2020.

the country had not put in place adequate safeguards to prevent duplication.

Some users expressed anger at the fact that the terrorist group, Boko Haram, was able to fraudulently obtain ID cards yet citizens were unable to obtain genuine ones. Aside from the delays, significant bureaucracy and corruption were noted as hinderances to obtaining the ID. Users complained of officials requesting bribes – a common phenomenon across all forms of ID surveyed. The absurdity of the situation is compounded by the fact that the ID cards in Nigeria, have an expiry date. Multiple users complained that with delays spanning years, most of their ID cards are issued after their expiry. This means that users have to apply for renewal and go through the same, long bureaucratic process. If that weren't enough, the NIMC charges a renewal fee that a few users complained of. Persons unable to get a national ID suffer considerably and are excluded from formal services. One post noted that a student was denied emergency health care due to not having an ID card on his person. In 2019, the Federal Government of Nigeria made in mandatory to have the national ID; failure to do so would attract penalties.[62]

For the passports and driver's licenses, users primarily complained about the corruption involved in obtaining these documents. Users would usually be required to part with significant sums of money in order to get a passport or driver's license. Even without this additional cost, the government-imposed fees were found to be high, effectively excluding poorer members of the community.

User posts regarding the BVN raised a new set of problems – privacy concerns and an absence of user control. Over half of the posts complained of clerical errors in their BVNs and long delays rectifying said errors.

More alarmingly, there were complaints of banks leaking customer data opening them up to scammers who often called pretending to be bank officials. There was also one user who explained that some officials request the BVN when one is applying for a national ID in order to check the applicants' account balance and request a bribe on that basis. This clearly indicates that BVN data is not siloed and access thereto uncontrolled.

Nigeria's ID ecosystem is flawed on numerous levels. At the core of the harms complained of is systemic fraud that perpetuates exclusion and robs users of any value they may derive from ID. The prerequisite of unlawful payments to obtain a compulsory ID along with the unjustified delays means that users suffer doubly – whether they choose to apply or not, it is not guaranteed they will have an ID.

h. SOUTH AFRICA

Prior to 2015, South Africa's ID was referred to as a 'book' and lacked any biometric features.[63] The country transitioned to a smart/electronic ID issued by the Department of Home Affairs (DHA). The ID, based on the Automated Biometric Identification System (ABIS), was rolled out over a 5-year period.[64] Both citizens and non-citizens are registered under this system. In 2009, the country also introduced an ePassport.

Users in South Africa primarily complained of the national ID, birth certificate, death certificate, marriage certificate and passport. Narratives indicate significant delays and long processes to obtain the e-ID. In a post, the Department of Home Affairs (DHA) stated that the issuing of an ID card can take up to 12 months. A user highlighted that temporary IDs (useful during the wait period) are obtainable at a cost – excluding those unable to afford it. Aside from this, queues at the DHA offices were observed to be a barrier. Five users complained of delays and bureaucratic processes to obtaining/rectifying birth, marriage and death certificates. Two users also complained of not being in the national database despite having IDs and being citizens. Similar complaints have been echoed in relation to passports with users observing excessive delays.

[62] https://punchng.com/fg-approves-mandatory-use-of-national-id-number-from-january-1-2019/ accessed 9 July 2020

[63] https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/south-africa-passport accessed 10 July 2020.

[64] http://www.dha.gov.za/index.php/civic-services/abis accessed 10 July 2020

In comparison to the other countries in the study, South Africa's ID ecosystem is relatively better. The main issue remains in the service delivery – delays and clerical oversight.

i. TANZANIA

Tanzania's current national ID issuance process began in 2013 with all citizens, residents and refugees above 18 years old eligible.[65] Each person is issued with a unique identification number on a smartcard with biometric functionality.[66] In accordance with its regional commitments, Tanzania recently began rolling out the EAC e-Passport. [67]

At the onset of Tanzania's national ID rollout, the WBG commented that the system was quite complex and technical. Other commentators also noted that the process was not uniform across the country. Approximately 96% of the identified posts relate to the country's national ID and the challenges that arose from the registration process. Half of these posts indicated inordinate delays in the issuance of the ID. Coupled with these delays was the poor service experienced at the various registration centres. Users also complained of having to contend with impending disconnection of their SIM cards where they failed to obtain IDs. Therefore, it would not be uncommon to find persons whose SIM cards have been disconnected for failing to obtain an ID, yet that failure is attributable to delays in the government's own process.

The remainder of posts relate to the EAC e-Passport. Much like the cancellation of SIM cards, users complained of the deadline placed on obtaining an e-Passport. This deadline was highly impractical as the national ID is required to obtain the passport; the issuance of the ID itself had been delayed for a large number of people. Aside from this, users complained of an overabundance of government issued ID – indicating a low amount of user value derived from each ID.

Majority of the harms reported in Tanzania relate to poor implementation of the ID systems. There were no identified reports of privacy violations or exclusion.

j. UGANDA

In 2015, Uganda enacted the National Registration of Persons Act and began to issue electronic IDs.[68] Recently, the country partnered with Mühlbauer to enhance registration across the country.[69] Much like Kenya and Tanzania, Uganda also began issuing the EAC e-Passport recently.[70]

75% of the 37 identified posts in Uganda related to the National ID issued by the NIRA. 14% of these indicated extremely long delays in issuance. Another 14% indicated clerical errors that were difficult to rectify. And a singular post highlighted corruption in the application process.

A smaller number of posts related to the passports. There were users who experienced delays when the country ran out of materials to print the old generation passports prior to its transition to the new e-Passport. One user's file was lost altogether meaning she was unable to obtain a passport.

Other posts detailed user experience with a telecommunications company. They encountered difficulties changing their details, precluding them from being able to make use of their SIM Cards. In one instance, the telecommunications provider mistakenly blocked a user's mobile money account.

Similar to Tanzania, Uganda's system appears to suffer from operationalisation issues more than it does systemic fraud and exclusion. However, there was a particular instance of fraud noted in relation to the country's Tax ID. One user noted fraudulent charges imposed by the revenue authority on his account. However, this may have been due to error.

[65] https://www.id4africa.com/2018_event/Presentations/PS2/1-2-2_Tanzania_Alphonce_Malibiche.pdf accessed 10 July 2020.

[66] https://www.id4africa.com/2018_event/Presentations/PS2/1-2-2_Tanzania_Alphonce_Malibiche.pdf accessed 10 July 2020.

[67] Alvar Mwakyusa, 'Tanzania: E-Passport Rush As Deadline Looms', AllAfrica, 6 January 2020 -< https://allafrica.com/stories/202001060490.html accessed 10 July 2020.

[68] GSMA, Digital Identity Country Profile: Uganda, 2019, 7 -< https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Uganda.pdf accessed 10 July 2020.

[69] https://dig.watch/updates/uganda-partners-muhlbauer-digital-id-cards

[70] https://www.immigration.go.ug/media/online-passport-application-procedures-e-passport accessed 10 July 2020.

k. ZIMBABWE

The current system of national ID in Zimbabwe began in 1996 and is a biometric card.[71] In 2018, the government initiated a Biometric Voter Registration drive to digitize election rolls and purge the potential for voter fraud.[72] However, aside from this, some have commented that little public information exists regarding the country's ID system.[73] As per the country's department of the Registrar General, all citizens above 16 years are required to obtain a national ID.[74] Zimbabwe also transitioned to an e-Passport in 2018.

Generally, the posts in Zimbabwe highlighted the following harms: instances of discrimination in application, exceedingly high costs to obtain certain documents and the difficulty of the process. In particular, the cost of a passport was noted to be exceedingly high.

[71] World Bank Group, The State of Identification Systems in Africa: Country Briefs, 2017, 60 -< http://documents1.worldbank.org/curated/en/298651503551191964/pdf/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf accessed 10 July 2020.

[72] The Engine Room, Digital ID in Zimbabwe: A case study, 2019, -< https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf accessed 10 July 2020.

[73] The Engine Room, Digital ID in Zimbabwe: A case study, 2019.

[74] http://www.rg.gov.zw/index.php/services/national-registration accessed 10 July 2020.

VT OMNES VNVM SINT