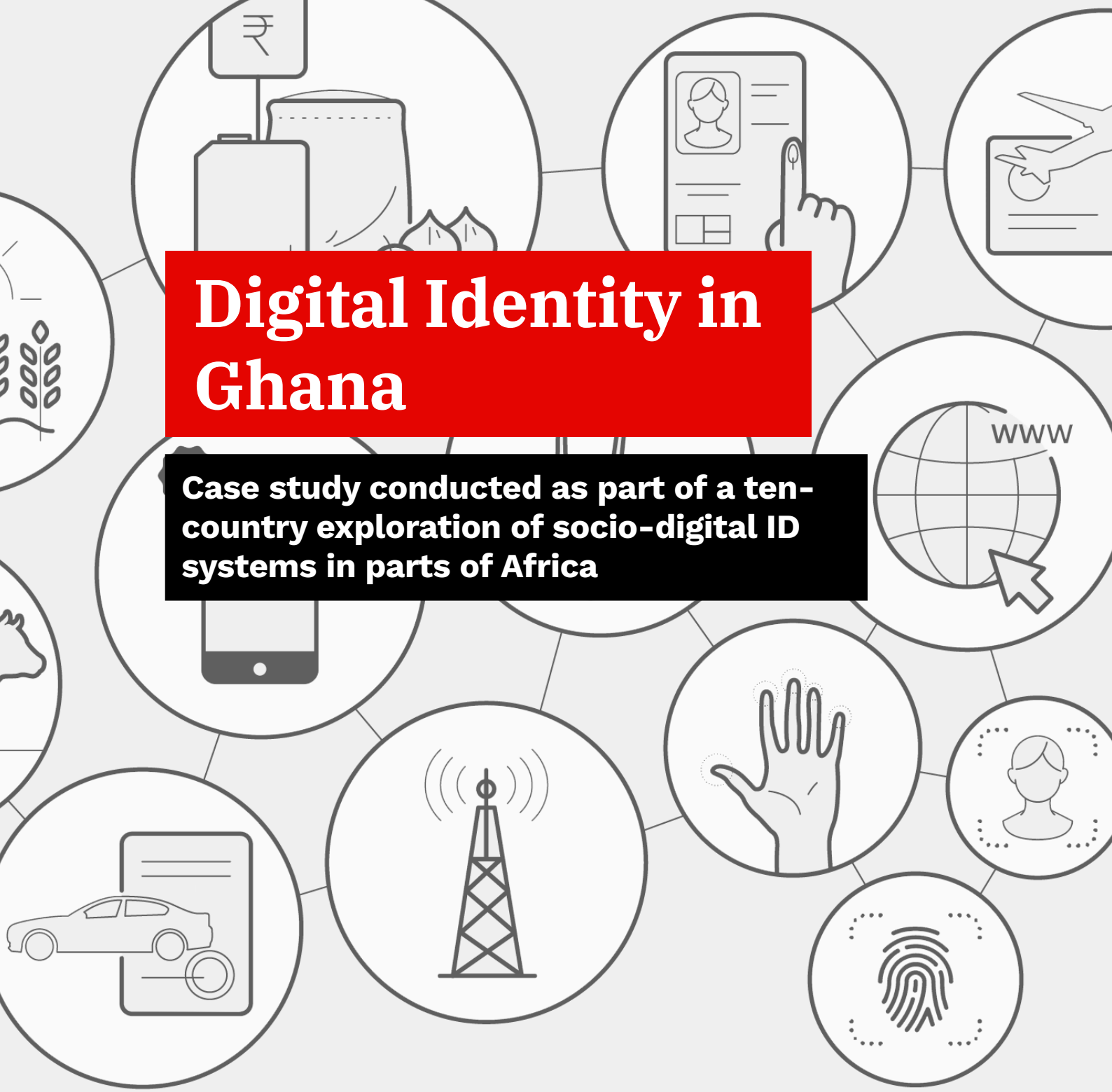


Digital Identity in Ghana

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

RESEARCH & WRITING
Smith Oduro-Marfo & Teki Akuetteh Falconer

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

COPYEDITING
Samantha Perry

COVER ILLUSTRATION
Akash Sheshadri

LAYOUT
Aparna Chivukula

RESEARCH ICT AFRICA

THE CENTRE FOR internet & SOCIETY

OMIDYAR NETWORK™

Digital Identity in Ghana

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

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

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

Digital Identity in Ghana

By Smith Oduro-Marfo and Teki Akuetteh Falconer, Africa Digital Rights Hub

PREAMBLE

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

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

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

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

2 Martin, Schoemaker, Weitzberg & Cheesman, 2021.

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

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

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

The Project

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

3 Breckenridge, 2014.

4 African Union Commission, 2021.

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

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

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

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

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

This report on the Ghana case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Smith Oduro-Marfo and Teki Akuetteh Falconer, Africa Digital Rights Hub. Besides being an independent case study, the findings from this report were also used to inform a comparative report put together by the RIA and CIS teams to analyse the similarities, differences, and other aspects across the ten case studies – including key recommendations for policymakers, researchers, civil society actors, and other stakeholders.

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

PREAMBLE REFERENCES

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

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

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

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

Press.

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

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

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

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

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

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

ACKNOWLEDGEMENTS

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

ABSTRACT

While there have been a number of prior studies on Ghana's national ID system, it is rarely framed and assessed as a digital ID. In this report, we highlight the digital components of the national ID and show how it increasingly fits the frame of a digital ID.

The report focuses on assessments of Ghana's ID from three main angles: first, we investigate whether the relevant laws pass the rule of law test in terms of their aim and mandate. Second, we assess whether the relevant ID laws are necessary and proportionate in terms of the rights that the use of the national ID may interfere with. Third, we track how well the risks associated with the use of the national ID were considered and mitigated by the National Identification Authority and also in the relevant laws, before citizen enrolment. We conclude with recommendations for the National Identification Authority, the Data Protection Commission, civil society bodies and donor partners.

Overall, we find that the legislative regime guiding the national ID system in Ghana is generally competent, especially as the Data Protection Act ensures that there are high standards for the collection, storage, use and sharing of personal data. We note that as the national ID project only recently finished a mass registration exercise, the challenges and success in using the system will become clearer in the next few years. An obvious danger, though, is that the increasing integration of the national ID with other databases deepens the potential abuse of the system for arbitrary surveillance. Also, the legislated mandatory uses of the ID means those without the card may be excluded from accessing certain services. Thus far, the main challenges have been impediments to enrolment, including the requirement of a digital address from enrolees, and claims that certain persons were prevented from enrolling because they were deemed not to be citizens. On the positive side, actions such as the zero cost of the card during mass registration, the government's decision to provide digital addresses for all homes for free, and the provision of a number of redress mechanisms for those challenging the use of their ID data are inclusive and do empower citizens in the context of the national ID. The potential excesses surrounding the national ID require civil society and the Data Protection Commission to be keenly alert, competent and rights-conscious.

ACRONYMS AND ABBREVIATIONS

CHRAJ	Commission of Human Rights and Administrative Justice
DPA	Data Protection Act
DPC	Data Protection Commission
ECOWAS	Economic Community of West African States `
NHIS	National Health Insurance Scheme
NIA	National Identification Authority
NIS	National Identification System
PIN	Personal Identification Number
ID	Identity Card
SSNIT	Social Security and National Insurance Trust
TIN	Tax Identification Number

CONTENTS

INTRODUCTION

1.1 THE CONTEXT

Ghana is a West African lower middle-income country with a population of about 30 million people. The country is generally touted as a good example of a stable democracy in Africa, marked by peaceful multi-party elections and inter-party transitions.

Traditionally, Ghana's ID space has been dominated by functional cards like the Voter's ID and the National Health Insurance Scheme (NHIS) card. The country has had challenges with developing an effective birth registration system and does not have a history of deploying a foundational national ID (Allan, 2015). Over time, different types of state-issued IDs have proliferated, a phenomenon we have described elsewhere as "card glut".[9] This card glut has often been due to the various state agencies that issue IDs maintaining a siloed approach as a way of retaining or hoarding the power and budgetary allocations associated with such ID projects (Falconer *et al.*, 2020).

In recent years, the Ghanaian state has shown more commitment to setting up a national ID system; to generate "one ID for all" that curbs the proliferation of state-issued IDs. The government and National Identification Authority's vision is to have an "integrated multi-sectoral and multipurpose National Identity System" (NIA, n.d.). This case study specifically examines this ID, namely the National Identification System (NIS). A mass registration exercise was completed in 2020 and as such, the national ID is still new in terms of adoption and use (Kasapa FM, 2021).

This work is part of a series of case studies, using the Centre for Internet and Society's Evaluation Framework for the governance of digital identity systems. These case studies, which analyse identity programmes and their uses, illustrate how the framework may be adapted to study instances of digital identity across different regions and contexts. The methods used for this report are mainly document analysis and legal analysis. Where clarifications were needed, we engaged key informants.

Ghana's National Identification System is intended to generate a population register of all Ghanaian citizens. It is meant to be a centralised foundational ID system that will eventually serve to validate enrolment in other functional

9 In a previous study, we mapped the various IDs in Ghana and the related actor relations. See map here: *https://kumu.io/CaribouDigital/ie-map-ghana*

registries.[10] The database is electronic and compiled, held and managed by the National Identification Authority (NIA), set up under the aegis of the Ministry of Communications and Digitalisation.[11] The national identity register has been built from scratch without relying on any prior existing register or database. As indicated later in this report, while we do not find any law that makes the national ID mandatory for citizens, there are mandated uses of the card.

Each citizen is to be given a biometric ID card, popularly known as the "Ghanacard", which is also a smartcard and has room for 14 different register applications, such as the e-passport application for the Economic Community of West African States (ECOWAS).[12] Thus, the Ghanacard can simultaneously host other state IDs like driver's licenses and voter ID. During enrolment, over 30 data points are collected from an individual, including biometric details such as prints of all 10 fingers, facial images, eye colour, hair colour and signature.[13] Each registered person gets a unique personal identification number (PIN), which is also shown on the ID card. By April 2020, about 15.5 million citizens had registered for the Ghanacard (representing about 52.5% of the population).[14]

The National Identity Register Regulations (NIR Regulations) provide that a non-citizen version of the ID can be accessed by permanently resident foreigners and by foreigners who reside in Ghana for a cumulative 90 days in a calendar year. Foreigners must pay USD 120 to enrol, unlike citizens, who do not have to pay for the card.

10 "A foundational identity system is a core Identity System created to manage identity information for the general public, and to provide identity proof for a wide variety of public and private services". "A functional identity system is designed to meet the needs of an individual sector, and is not designed for, though, in some cases, may be used for other purposes or in other sectors". See CIS-India (n.d.)

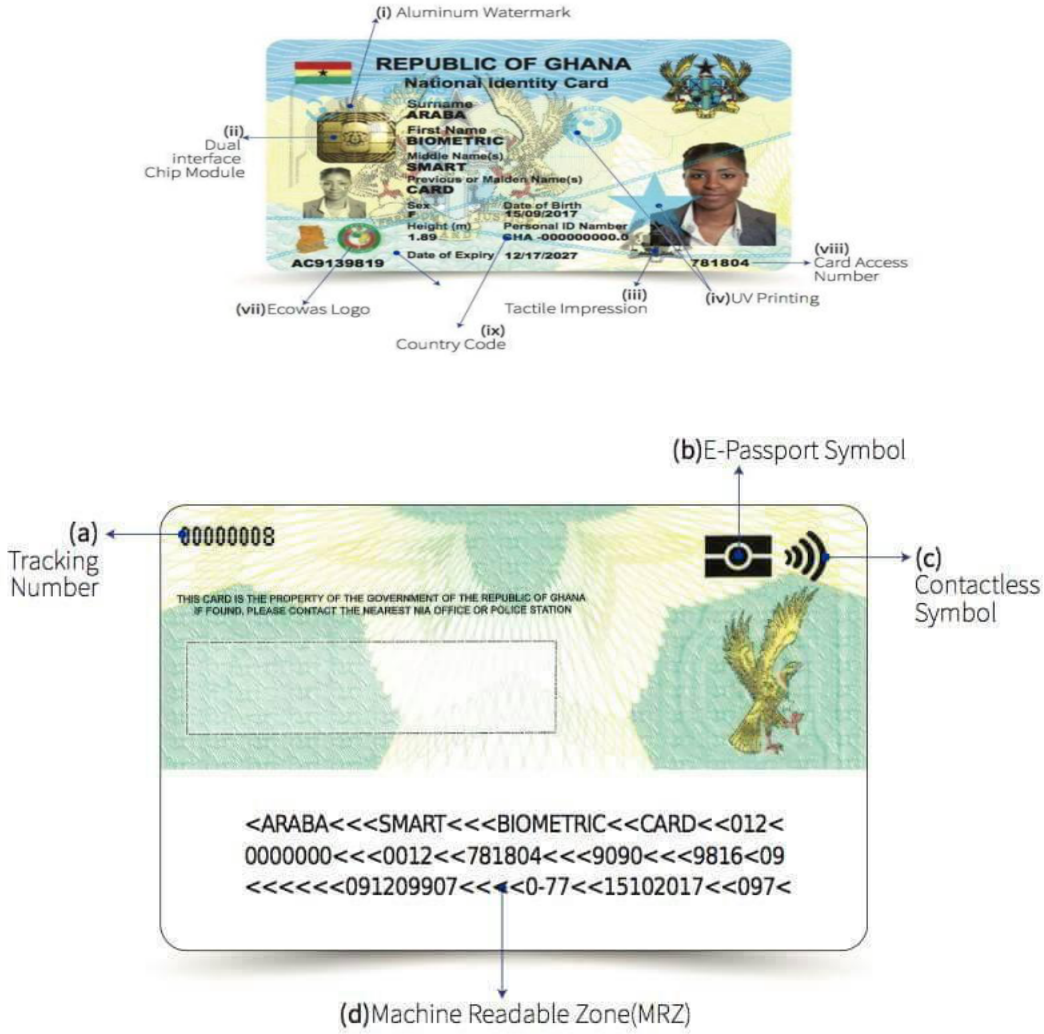
11 Per our checks, the NIA is being moved from the oversight of the Ministry of Monitoring and Evaluation under the Presidency.

12 The ECOWAS as a sub-regional body is encouraging its members to have a common passport. Ghana's national ID is designed to also serve this function as an ECOWAS passport.

13 The full list of citizens' personal data to be collected can be found both in Section 4.2 of the NIR Act and Section 1 of the National Identity Register Amendment Act.

14 The NIA has communicated that its registration target is 16 million citizens out of the 30 million general population. The discrepancy is accounted for by the underaged (younger than 16) population, who are not given the Ghanacard. See NIA (n.d.) and Citi Newsroom (August 2020)

Figure: Ghana's National ID Card[15]



Unlike countries like India, Nigeria, and Kenya, Ghana does not currently have a standalone digital identity project. Ghana's national ID is a physical card that contains a personal identification number (PIN), biometric information and other personal details. Typically, its use is thus mostly physical and in the context of visual checks and card scans. In this sense, the manner in which the NIN in Nigeria, Aadhaar in India and Kenya's *Huduma Namba* immediately lend themselves to the tag of "digital identity" is not replicated in Ghana.

However, as a biometric smart card, the Ghanacard has digital credentials

15 See Mybeeponline (n.d.)

and utilities. The card, for example, holds citizens' digital images, signatures and fingerprints. It also has a memory chip that can hold about 14 different ID applications. The Ghanacard is designed to simultaneously hold the IDs of various functional state agencies, such as those of the Driver and Vehicle Licensing Authority and the Electoral Commission. The database of all IDs and their associated personal information as held by the NIA is electronic. The tracking number at the back of the card is used to certify or whitelist the card for recognition by personalisation software. Increasingly, the digital utility of the Ghanacard is becoming more pronounced. For example, the Ghanacard PIN is being linked to other registries like the NHIS and the Social Security and National Insurance Trust (SSNIT) (CBN, 2021; ISD, 2020). The government is also attempting to make the Ghanacard PIN function as a citizen's Tax Identification Number (TIN) (GRA, 2021). A concern with this policy is how it excludes citizens who have not accessed the national ID yet and also do not have existing TINs. As citizens Ghanacard PINs are being tied to government and private services, it could quickly gain the stature of ID numbers in countries like Kenya, Nigeria and India.

While the Ghanacard idea has been present since 2006, the project is only recently seeing success in terms of registering citizens and providing them with IDs. Thus, its use is relatively new, and as such, its practical challenges and successes are likely to be clearer in the next few years. As discussed later, the process of operationalising the national ID project in Ghana has revealed challenges such as the potential exclusion of certain persons from enrolment. This is due to the requirements of a digital address during enrolment and the claimed uncertainty of the citizenship of some persons attempting to enrol.

RULE OF LAW TESTS

2.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

The national ID project in Ghana is backed by validly enacted laws to be a proof of citizenship. It is not explicitly legislated as mandatory ID for citizens, but citizens without the ID could be denied the services that by law require possession of the ID. The National Identity Register Act, 2008 (Act 750) established the national identification system/register.[16] The register is the electronic database that contains data on citizens. It is only those on this roll that are given the Ghanacard.

The NIR Regulations, 2012 (LI 2111) provides modalities for compiling and using the register.[17] The National Identity Register Amendment Act, 2017 (Act 950) expanded the data points to be collected from enrolees, to include a digital address, for example.[18] The Amendment Act also disqualified voters' IDs from being used as proof of citizenship during enrolment on the basis that Ghana's electoral roll was not reliable, as foreigners had been fraudulently enrolled onto it in the past (Starr FM, 2018). The Amendment Act made the submission of a digital address a requirement for accessing the national ID. The digital address is akin to a GPS code that identifies the location of one's residential facility. Thus, the requirement is a challenge for the homeless and those without internet or smartphones. However, the government has embarked on a project of national address generation and tagging for all residential facilities. Of course, this intervention still does not resolve the challenge faced by homeless persons.

The law to make a digital address compulsory for enrolling for a national ID has been challenged in court by a private citizen on the basis that the requirement undermines existing citizenship (GNA, 2019). In short, the case considered why a citizen should have a digital address, a very recent innovation in Ghana, before being given a national ID card. A High Court judge dismissed the case, deeming the substantive question as one that the Supreme Court should rather address, but it also added that discrimination was not a concern where there had been no evidence that enrolees have been registered without the digital address (ibid.). In effect, the real question of whether one's access to a national ID must be subject

16 Find a copy here: *https://www.refworld.org/docid/548ee10b4.html*

17 Find a copy here: *https://www.nia.gov.gh/registration_act.pdf*

18 Find a copy here: *https://nia.gov.gh/act_950.pdf*

to submitting a digital address remained unanswered by the court. Currently, citizens must provide their digital address, or they cannot access the national ID.

QUALITY OF LAW

If the quality of law is chiefly understood as an element that allows for Section 7 of the NIR Regulations specifies the mandatory uses of the Ghanacard.[19] Section 7(1)(n) of the Regulations also permits the NIA to determine additional transactions for which the ID is required. Such discretionary powers of the NIA are rather substantial and may be used to legalise mission creep, but this has not happened yet. A particular challenge is that while the IDs have biometric data and PINs, the alternative reimagination of the Ghanacard as a digital ID and not as physical cards is hardly present in the laws. This means that even 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. For example, there have hardly been any engagements about whether the use of PINs may require service providers to use hashing techniques as a security and privacy safeguard.

On a positive note, the Data Protection Act (DPA), enacted in 2012, might be applied to deal with any potential gaps in the existing ID laws, specifically related to data protection. Generally, as PINs and biometrics are all considered personal information, their collection, use and disclosure are regulated by the DPA, 2012 (Act 843).

CLARITY AND PRECISION OF LAW

While the ID laws are generally precise and clear, they do grant subjective powers to various state actors. For example, in the National Identity Register Act (NIR Act), the responsible minister can make further regulations to facilitate the enforcement of the Act. The responsible minister (on the advice of the NIA board) for instance, has the power to "provide that every public office should demand the presentation of an identity card as a condition precedent to the provision of its service".[20]

Additionally, in terms of the contents of the national ID register, the responsible minister could use regulations to require the submission of further personal information by citizens.[21] Thus, the law is clear on who has the power to make

19 These include application for and issuance of a passport, driver's license, personal bank account, insurance policy, SIM card; registration for voting, national health insurance; and the payment of taxes. See NIR Regulations, LI 2111 of 2012, Section 7.

20 See the NIR Act, Act 750 of 2008, Section 73 (1)(f).

21 See the NIR Act, Act 750 of 2008, Section 4(2)(d).

subjective determinations, but such discretion means citizens lack clarity about which new information may suddenly be required beyond existing law, and which new user agencies could make the ID a requirement for accessing their services. In essence, the responsible minister has almost infinite power to determine what information or data should be collected and who can be a user agency, without sufficient checks and balances. Thus far we do not observe any invocation of the aforesaid powers by the sector minister, and that is likely due to how expansive the legislated or mandated uses are already. Notwithstanding, it is noteworthy that in Ghanaian law-making, the scrutiny of parliamentary bills tends to be stronger than that accorded to instructions and regulations made by ministers.

2.2 LEGITIMATE AIM

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

While the aim of the ID is not explicitly spelled out in the various pieces of legislation, it can be inferred from the objectives of the NIA as provided in the NIA Act, Act 707 of 2006, Section 2(1). This Act establishes the NIA, with its object being to create, maintain, provide and promote the use of national identity cards in order to advance economic, political and social activities in the country. The objective/aim of the ID thus is generally legitimate. The project's goal is also non-discriminatory, as all citizens are supposed to be registered. Non-citizens designated as permanently resident in Ghana or having resided in Ghana for at least 90 days in a year can also access the card (NIA/b, n.d.).

2.3 DEFINING ACTORS AND PURPOSE

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

Section 7 of the NIR Regulations mandates the activities for which the national ID is required.[22] These include registration for passports, health insurance and bank accounts. While user agencies are not specified by name, a number of the mandated functions are only performed by certain specific bodies.[23] For example, the Ghana Revenue Authority is responsible for tax collection; the

22 See footnote 5.

23 Per Section 75 of the National Identity Register, a user agency is an entity "which requires identity data from the [National Identification] Authority".

Lands Commission is responsible for the registration of land titles; the Electoral Commission is responsible for registering voters; and the Passport Office issues passports.

Importantly, the listed mandated functions suggest that not only public user agencies can require the national ID, but certain private user agencies can demand it too. For example, the functions for which the ID is required also include privately-provided ones such as opening a bank account, purchasing insurance policies, registering for a SIM card, and various consumer credit transactions. Thus, private actors which depend on the national ID to deliver their services are mandated to demand the national ID when providing services captured under Regulation 7 of the NIR Regulations. It is noteworthy that the NIA, in Section 7(1)(n) of the NIR Regulations, can supplement the functions for which the national ID can be required, thereby also expanding the number of user agencies. Thus, per the law, private and public agencies must be providing one of the services provided for in the regulations or by the NIA to require the national ID.

One challenge is that while public and private user agencies are mandated, there is no stated differentiation in their rights and obligations. The discretion granted to the NIA also fosters uncertainty about the services for which the national ID is required and the user agencies that can require the national ID before providing services. Overall, it is important that room is made in the law for accessing the listed mandated services where one has a different but viable means of proving citizenship. So far, the national ID (as proof of identity) is being used alongside other IDs, like the passport. However, it is more valuable if this openness to multiple proofs of identity is backed by law.

2.4 REDRESS MECHANISMS

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

In terms of notifying data subjects, there are legal obligations under the NIR Act; NIR Regulations (in its attached Form 3); and the DPA (2012) on issues such as user agencies seeking consent before collecting or accessing an individual's data (Sections 23 and 25); the notification of security breaches (Section 31); and the need to seek consent before secondary use (Section 25).

In the NIR Act, the NIR Regulations and the DPA, certain provisions permit individuals access to their data as well as the right to the correction of inaccurate personal information both at the NIA and user agency level.[24] But there are caveats limiting such access and correction, including: when the information is

24 See Sections 32-35 in the DPA; Sections 51 and 52 of the NIA Register Act; and Regulation 14 of the NIR Regulations.

tied to another person's information who has not provided consent for access or correction; confidential information that would affect the interest of the authority; investigations; and where ID information relates to a breach of or a contravention of law that has been, is being or is about to be committed.[25] For instance, if someone wanted to have information from the NIA on how their card has been processed by a user agency, certain aspects of the information that would reveal the personal information of others may have to be held back if the third party has not consented to the release of their information. Similarly, if such a request would undermine national security or ongoing criminal investigations, the NIA can refuse the request.

If aggrieved by the NIA, a data subject can complain to the NIA and can compel the NIA to grant the opportunity to rectify its actions and decisions if deemed necessary. However, complainants who are dissatisfied can appeal to the Commission of Human Rights and Administrative Justice (CHRAJ), followed by the High Court and finally the Court of Appeal.

For data privacy breaches, including unauthorised collection, use and disclosure of personal ID information, the DPA can be invoked by aggrieved parties. The DPA directs data subjects to complain first to the data controller and, if unresolved, appeal to the Data Protection Commission. Overall, these are viable opportunities for seeking redress on issues related to the use of a citizen's ID data. While these avenues for redress should be sufficient in theory, in practice their effectiveness would always be shaped by citizens' awareness of their existence, and trust in the systems, in addition to judicial commitment.

2.5 ACCOUNTABILITY

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

The DPA guides the collection, storage, use and disclosure of personal information by all data controllers and data processors. The Act then serves as an accountability mechanism guiding the use of the national ID. For instance, Section 17 of the DPA obliges processors of personal information (in this context, user agencies) to ensure "accountability, lawfulness of processing, specification of

25 See Section 51(b) of the NIA Register Act and Sections 32-35 of the DPA.

purpose, compatibility of further processing with purpose of collection, quality of information, openness, data security safeguards, and data subject participation". The NIA and any other public and private actors that collect or process national ID information are subject to the provisions of the DPA, because they are dealing with personal data.

In terms of financial accountability, the NIA is subject to the Auditor General's oversight. The Auditor General tracks the finances of various state and governmental offices and agencies and could demand resolutions and corrections where financial misappropriation is seen.[26] The NIA must also submit an annual report to the Parliament of Ghana detailing its activities and decisions.[27]

In terms of the use of the national ID, certain provisions in the National Identity Register Regulation and the NIR Act also provide accountability measures. For example, the provision for data subjects to complain to CHRAJ, the High Court, the Court of Appeal or the NIA about their grievances relating to uses of their ID by user agencies or by the NIA serves as a system of accountability.[28] The Personal Information Sharing Agreement Form (in the annex to the NIR Regulations) similarly guides the transfer of personal information between user agencies and holds user agencies accountable for the personal ID information they access. For example, the receiving agency must expressly commit to be accountable for the personal data and the specific purpose for collecting the data must be specified.

Overall, the accountability options are viable and useful, especially as the DPA supports the relevant ID laws by deepening the general accountability that must accompany the collection, use and disclosure of personal information.

2.6 MISSION CREEP

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

Both the NIR Act and the DPA permit the collection of personal information only for stated purposes. While the NIR Act does not provide for remedies in instances where the NIA goes beyond its purpose, it provides that aggrieved persons could take up their grievances with the NIA, followed by the CHRAJ, then a High

26 See Section 15 of the NIA Act.

27 See Section 16 of the NIA Act.

28 See Regulation 19 of the NIR Regulations; and Section 62 of the NIR Act.

Court, and finally the Court of Appeal, in that order.[29] The DPA also provides an opportunity for data subjects to complain to the Data Protection Commission if data collection or use goes beyond its stated purpose.[30]

Practically, the services that, by law, require the national ID seem very expansive, and as such the various linkages to the card are already covered by existing law. However, it must be noted that the legislative discretion granted to the responsible minister and the NIA means that any subjective addition of mission could be justifiably legal once the responsible minister places it in a regulation or the NIA puts it in gazette. Overall, it will be useful to curtail the discretion granted to the minister and the NIA such that any additional service to require the national ID may only be permitted once it is legislated. This approach would allow some more substantive debate before the provision is mandated.

29 See Regulation 19 of the NIR Regulations

30 See Section 77 of the DPA

RIGHTS-BASED TESTS

3.1 NECESSITY AND PROPORTIONALITY

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

As the central goal of Ghana's ID system is social and economic progress, the identification, verification and authentication of personal information for such a purpose is permissible. Citizens also generally benefit from better delivery of the legislated services for which the use of the ID is mandatory, including SIM registration, accessing health insurance, and opening a bank account.

It is, however, important that accessing such services is not rigidly and mandatorily tied to the national ID, especially as there are other IDs (including passports and voter IDs) which should be adequate proof of citizenship and identity. Overall, the existence of the DPA means that in theory and in law, privacy is generally protected through principles such as the need for purpose-specified collection and use, use limitation and data minimisation.[31] Generally, these provisions in the DPA should be sufficient to ensure that data collection, disclosure and use as related to the national ID meets the principles of necessity and proportionality.

A potential problem is the exceptions to consent for processing a national ID. In effect, there are situations in which a citizen's national ID can be processed without the person's consent, and this may not be related to any of the services for which the ID is required.[32] Section 21(2) of the DPA provides such exceptions, including national security and where "compliance is not reasonably practicable". Section 49 of the NIR Act similarly provides exceptions to consent, including national security concerns and "for a purpose relevant to the functions of the [National Identification] Authority". The danger here is that what constitutes "national security" or where compliance is not practicable or relevant to the purpose of the NIA, may be so subjective such that it could lead to unwarranted privacy violations.

31 See Sections 22, 25 and 19 of the DPA.

32 Where the ID is required, one may withhold consent and forfeit service. But within the bounds of the exceptions, nonconsensual use of a person's ID is permitted.

3.2 DATA MINIMISATION

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

The DPA calls for the collection of only data that helps in the performance of a specified purpose.[33] Yet, the NIA by law, requires over 30 data points to be collected during Ghanacard enrolment, including height, eye colour and marital status.[34] In reality, a number of the 30 data points are things that citizens are not obliged to have, such as other state-issued IDs. In that sense, not all of the 30 data points may actually be obtained from an enrolee. Thus far, the only data point out of the 30 that has been challenged in court is the digital address. As mentioned in Section 1.1 above, this case did not lead to a repudiation of the digital address as a requirement. However, the collection of all these data points can increase the risk of surveillance and data breach. Some of these data points, like marital status and email address, are unnecessary for a national ID.

In terms of processing, Section 19 of the DPA instructs that "personal data may only be processed if the purpose for which it is to be processed, is necessary, relevant and not excessive". In addition, the Personal Data Sharing Agreement form provided in the NIR Regulations includes a section where an agency requesting ID information must specify the personal information needed, and for what purposes. The same form does not permit secondary uses of accessed personal data "except with the consent of the individual concerned or as permitted by law" (ibid).

However, it is unclear how long the accessed data can be stored by the user agency after serving its purpose. While the NIR Act indicates that the retention period will be indicated in guidelines released by the NIA, no such guidelines have been published. Although the DPA provides in its Sections 24 (5) and (6) that personal information must be deleted after the required retention period, none of the relevant ID laws mentions a right to deletion. The mandatory nature and use of national ID registration could explain why a right to deletion is absent in the context of the NIA and for some user agencies, like the Ghana Revenue Authority. However, it should be viable for the deletion provisions in the DPA to cover user agencies whose services are not perpetual such that retaining information when its purpose has been served is unnecessary.

33 See Section 19 of the DPA.

34 See Section 1 of the National Identity Register (amendment) Act

3.3 ACCESS CONTROL

Are there sufficient protections in place to limit access?

The DPA, Sections 53-61 of the NIR Act, and Regulations 15-18 of the NIR Regulations regulate access to ID data by user agencies. To be clear, designating a body as a user agency is more about the functions it performs than whether it is public or private. While many of the mandated transactions may be performed by public bodies, once an entity's work is listed as one of the transactions that require the card, it is a user agency.

User agencies accessing ID information from the 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.[35] If the ID information is not being requested from the NIA, the user agency must have the consent of the individual in question, and the use must not be prejudicial to the "interest of the individual" whose information is being sought.[36] Certain caveats, however, provide for instances where an individual could be denied their access rights. This includes where such access could undermine ongoing investigations or national security.[37] And while specific provisions guiding the access of the NIA to the register are absent, the NIR Act provides in Sections 66 and 67 that unauthorised access and modification of the personal information held on the NIA's "computers" is an offence punishable with "summary conviction to a fine" or to a "term of imprisonment of not more than [10] years or to both". In this sense, unauthorised actions within the NIA may be punishable by law. However, it will be useful to have explicit transparency about the access rights and restrictions within the NIA.

3.4 EXCLUSIONS

Are there adequate mechanisms to address exclusion from the system?

Two aspects pertaining to exclusion are relevant to the Ghanaian case. The first relates to exclusion from accessing the ID. The second is exclusion pertaining to the consequences of not having an ID and thus access to certain public and private services.

35 See Regulation 15 of the NIR Regulations

36 See Sections 53 and 54 of the NIR Act

37 See Section 51 of the NIR Act

In respect of the first type of exclusion, the national ID is free to access (citizens do not have to pay to have it), and every citizen has a right to access the ID by law. The NIA also visited communities during its mass registration phase, and is launching offices in all 275 districts in Ghana to have a stable and decentralised presence around the country (Jacobs, 2021). These measures promote inclusiveness in terms of access to the national ID. It must be noted, however, that the non-citizen card costs USD 120. There have been some complaints by a section of the migrant community about the cost and even utility of a non-citizen card, as they hold other identity documents like their passports (Nyabor, 2019).

Citizens can also invoke certain legal provisions to enforce the right to a legal identity. While registration officers and citizens could challenge a person's enrolment on suspicions of non-citizenship, Sections 22-27 of the NIR Act, provide for persons whose registration has been officially challenged to seek reviews from the district level to the High Court if dissatisfied.[38] However, some persons have expressed concerns about being turned away from registration centres based on suspicions that they are not Ghanaians (Starr FM, March 2020). Such complaints have mainly been from Fulani people and members of Zongo communities.[39] It is important to note that procedurally, registration officers are not allowed to turn away enrolees they are not sure about, but should allow enrolees to fill in a challenge form.[40] While these non-registration concerns have been raised publicly, there is no public reporting on whether individuals resisted their non-registration officially or, if they did, what the outcome or the official resolution on the matter was. Making such official resolutions public could build up public trust in the inclusiveness of the NIA's measures.

In respect of the second type of exclusion, the mandatory uses of the ID as prescribed in Section 7 of the NIR Regulations are relevant in themselves. However, such mandatory uses mean citizens without the national ID might miss out on the related public and private goods and services. As indicated before, the question that remains is whether, in such cases, an alternative proof of identity (if provided by citizens) should suffice. Existing laws are also silent on what happens in cases where a person has the ID, but authentication is not possible or is challenged. In the meantime, the ID requirement for services under Section 7 of the NIR Act has largely not been rigidly enforced.

38 Section 5 of the National Identity Register (Amendment) Act amends and extends the last court of review to Court of Appeal.

39 Traditionally, the Fulani are a nomadic and transhumant group and as such have had issues in proving their roots in various West African countries. The Zongo traditionally tends to be a settlement for various (often Muslim) immigrants from across West Africa including Niger, Mali and Nigeria. However, it is unwieldy to suggest that all members of Zongo communities are immigrants.

40 See Section 22 of the NIR Act.

Curiously, in the meantime, banks are reportedly refusing to accept the national ID on the basis that the ID is not yet verifiable (Yeboah, 2021). This inability to verify the national ID is mainly because there seems to be no "final" database against which a person's national ID can be checked (ibid.). Banks are still accepting the passport, driver's license and the Social Security and National Insurance Trust ID (ibid.). While refusing the national ID may go against the law and potentially exclude from banking persons who only have that ID, the banks are also proving the possibility of eventually allowing multiple IDs to be used as proof of identity.

3.5 MANDATORY USE

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

Section 4 of the NIR Act mandates the NIA to register every Ghanaian citizen. The national ID register is conceived as a population database. However, a direct provision that makes enrolment for the national ID compulsory for citizens is absent in Ghana's ID laws. Because accessing many critical services is, by law, tied to the national ID, there is a sense of compulsion in having the national ID or facing the possibility of losing out on crucial services if the current law is rigidly enforced. Section 7 of the NIR Regulations lists the services for which the card must be provided, including registering for a SIM card, a bank account and a land title.[41] The power to determine these mandatory uses is granted to the responsible minister in Section 73(f) of the NIR Act. The NIA can also add to these mandatory uses per Section 7(n) of the NIR Regulations.

Overall, Ghanaians may not be obliged to register for the national ID and, as such, there are no legal provisions against or any punishment for refusal to register. However, the freedom to not register is seriously undermined by the mandatory uses. So far, no citizen has been punished for not registering for the national ID, and other IDs (such as the passport and voter's ID) are being accepted by various service providers. Generally, this may be because the government and the NIA seem to be approaching the present period as one for instituting the ID system.

41 See footnote 5

RISK-BASED TESTS

4.1 RISK ASSESSMENT

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

Our research did not reveal any risk assessment reports on the ID as related to privacy harms, rights breaches and exclusion. However, the provisions in the relevant ID laws on privacy rights, data correction, data accuracy and breach notifications suggest some initial understanding of potential data privacy risks related to the national ID.

Again, there is no charge for enrolment and redress mechanisms (including challenging the NIA's decisions and registration challenges), which suggests some initial consideration of risks by policy makers. Also, where a person does not have a relevant ID to register for the national ID, provision is made for people possessing the national ID to vouch for the former.[42]

A comprehensive risk assessment could do more to show the depth and breadth of potential risks with the national ID system as they relate to privacy, rights and exclusions. For example, to meet the requirement of a digital address during enrolment, individuals could generate a digital address anywhere and present it falsely as the coordinates for their home. This could challenge the accuracy of the register and undermine its utility, but there are no clear safeguards put in place by the NIA against this practice.

4.2 DIFFERENTIATED APPROACHES TO RISK

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

The ID laws and regulations do not differentiate between the mandated uses as harmful or not, and as such do not specifically regulate potentially or actually harmful uses of the ID. The mandated uses in Section 7 of the NIR Regulations do not consider differentiated risks. Additionally, the laws and regulations do

42 See Section 8(2) of the NIRA

not provide for alternative means of proving identity. The risk that is provided for tends to be about ensuring that an individual's access rights (regarding information about how their ID is being used) do not undermine national security or ongoing criminal investigations.[43] In this sense, there is a consideration of the security risks, but from the perspective of the state and society, and not necessarily from the purview of individuals.

4.3 PROPORTIONALITY

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

Certain provisions in the NIR Act and the DPA allow for personal information to be corrected where necessary. The NIA and registered persons are both, by law, expected to ensure that ID information is accurate.[44] Section 67 in the NIR Act criminalises the unauthorised modification of ID details. In this sense, some room has been made for a governance regime that ensures that the risks of inaccurate ID data can be reasonably mitigated.

The relevant ID laws do not address the issue of authentication errors. The closest provision is in Section 9 of the NIR Regulations, which provides that where a legitimate entity believes that a physical ID is false, they could use a biometric scanner to verify and authenticate the ID. Indeed, the processing of the PIN and the biometric data associated with the national ID means that there could be issues with authentication and, as such, it is necessary that there is more legal clarity on how authentication risks must be governed.

Section 15 in the NIR Regulations mandates that user agencies specify the purpose for accessing data. The template Form 3 in the annex of the regulations prohibits agencies from using ID data for secondary uses without consent. The DPA also requires that personal information be used for the stated purposes when the information is collected.[45] These laws ensure that ID information is not collected or used indiscriminately.

The CHRAJ, the High Court and the Court of Appeal have been identified as outlets for individuals to challenge the NIA and user agencies in terms of how ID information is handled. Importantly, Section 70 of the NIR Act provides for

43 See Regulation 14 of the NIR Regulations

44 Per Sections 46 and 37 of the NIR Act, respectively.

45 See Section 22 of the DPA

punishing any person or entity breaching the Act.[46]

These aforesaid safeguards, including mechanisms for redress and punishment, generally indicate that the collection and handling of ID information is treated with caution and seriousness. They also suggest the appreciation of possible challenges, mishaps and criminal activities relating to the national ID and, consequently, lawmakers have put in place proportional governance measures to mitigate such risks and threats.

4.4 RESPONSE TO RISKS

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

To a reasonable extent, options to mitigate risks have been provided for in Ghana's ID laws. For instance, at the enrolment phase, the possibility of an erroneous challenge to a person's registration may be mitigated by the provision of a review process which could be pursued as far as the Court of Appeal.[47] Also, the risk that a person may not have any relevant ID to prove identity during registration is mitigated by the provision that the person's relative, or two registered persons, can vouch for them (NIA/c, n.d.).[48] These measures support inclusiveness in accessing the national ID.

In terms of ID use, user agencies are legally empowered to verify biometric details of an ID where they deem it to be suspicious.[49] In terms of an individual's access rights, there are provisions that support the NIA in not denying individuals' access to their personal information. The basis for such refusal includes where the NIA believes that disclosure could be used to contravene the law, or disclosure could inhibit investigations or undermine national security.[50] In terms of incidence of unauthorised use of or access to ID information, Section 31 of the DPA provides for a process that includes the data controller notifying the data subject and the Data Protection Commission.

46 Sections 65-69 of the NIR Act specify offences relating to the national ID database. These include obstructing the work of the NIA, and the unauthorised access to, communication and modification of the NIA's database.

47 See Sections 22-27 of the NIR Act

48 NIA/c (n.d.). Rules and Regulations. *https://nia.gov.gh/registration-rules-and-Regulations/*

49 See Regulation 9 of the NIR Regulations

50 See Regulations 16-17 of the NIR Regulations

While the foregoing measures are useful, there are still concerns about risks including the acceptability of data matching' what should happen when there are authentication errors, or what should happen if one applies for a mandated service, and does not possess the national ID but another valid state-issued ID. If user agencies decide to rigidly implement the law, there is a high risk that citizens who do not have a Ghanacard could miss out on critical public and private goods and services.

CONCLUSION

Overall, Ghana has a useful set of laws and regulations governing its national ID. These laws are further strengthened by the existence of the DPA. It is noteworthy that the NIA and the Government of Ghana have pursued inclusive options, such as embarking on a mass registration exercise from community to community, making the Ghanacard free, setting up an NIA office in every district and allowing others to vouch for the citizenship of enrolees when the latter do not have the requisite proof of identity. The NIA even provided a commissioner of oaths at each registration centre to ensure that such vouching can be done (Jafaru, 2018). It was also useful that, following public complaints, the Government of Ghana chose to embark on a nationwide digital addressing project to ensure that citizens would not be hindered during Ghanacard enrolment.

However, it is still challenging for the homeless and persons living in slums to have a reliable digital address. In that sense, there is the threat of certain persons submitting inaccurate digital addresses that could impede the accuracy and reliability of their profile details (Class FM, 2018). In truth, the digital address should not even have been obligatory when enrolling for the Ghanacard.

Some level of seriousness is attached to issues relating to the handling and processing of the national ID. What is lacking, however, is an explicit recognition of the national ID as a digital ID, and consequently a more direct approach to its peculiar implications. For example, having the national ID at the heart of the increasing interoperability of the databases of various public and private agencies means that there could be risks with data matching, authentication errors and non-hashing of the PIN. Such integration and interoperability provide a powerful surveillance tool that can be used by the state and other actors to undermine citizens' rights, especially where data protection laws are disregarded.

To conclude, we recommend that the NIA develop a dedicated policy document on the prevention, mitigation and resolution of risks to do with the digital components of the national ID.

We also recommend moving away from the mandatory uses of the national ID to a legislation framework that explicitly permits the use of other state-issued IDs if citizens do not possess the national ID.

Also, we recommend a more public resolution of the complaints of exclusion levelled by certain sections of Ghanaian society such as the Fulani and Muslims in some Zongo communities. Such a public resolution is important as it legitimises the NIA as an inclusive entity. Right now, it is not too clear whether persons who complained about being excluded from registration utilised the laid down complaint process, and if so, what the results were.

It is critical that the Data Protection Commission assumes a more public-facing role in creating awareness about privacy-preserving practices and mechanisms as they relate to the national ID. This must be accompanied by stronger and visible enforcement of ID laws by the NIA, the Data Protection Commission and the courts in Ghana.

Importantly, civil society actors must maintain a persistent interest in tracking the work of the NIA, user agencies and the Data Protection Commission, and in holding them accountable. This is necessary as the increasingly digital world means that the rights, freedoms and interests of citizens are progressively tied to the collection, use and sharing of the personal information of citizens. Donor agencies that promote digital ID systems in Africa, such as the World Bank Group, must 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.

REFERENCES

Allan, E. (2015). An Identity for Every Child: Birth Registration and Equity in Ghana. FXB Center for Health & Human Right. *https://fxb.harvard.edu/2015/03/18/an-identity-for-every-child-birth-registration-and-equity-in-ghana/*

CIS-India (n.d.). Digital ID – Core Concepts and Processes. *https://digitalid.design/core-concepts-processes.html*

Citi Newsroom (August 2020). Ghana Card mop-up due to failure to meet 80% target – NIA

Modern Ghana. *https://www.modernghana.com/news/1024506/ghana-card-mop-up-due-to-failure-to-meet-80-targe.html*

Class FM (2018). Ghana Card: People borrowing digital address to register. *Ghanaweb*. *https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Ghana-Card-People-borrowing-digital-address-to-register-699021*

Falconer, T.A. et al. (2020). Ghana's Identity Ecosystem Report. *https://africadigitalrightshub.org/wp-content/uploads/2020/10/Ghana-Identity-Ecosystem-Report.pdf.*

GNA (2019). Court endorses NIA's demand for digital address code. *Ghanaweb*. *https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Court-endorses-NIA-s-demand-for-digital-address-code-740836*

GRA (2021). Commencement of the use of Ghana Card Personal Identification Number as Taxpayer Identification Number. *https://gra.gov.gh/news/portfolio/commencement-of-the-use-of-ghana-card-personal-identification-number-as-taxpayer-identification-number/*

ISD (2020). Following Integration of the Digital Platforms. *https://isd.gov.gh/topstories-isdnews-authentic-government-news-at-every-corner-of-the-nation/777/*

Jacobs, D.P. (2021). NIA to open regional and district offices by June 2021. *Citi Newsroom*. *https://citinewsroom.com/2021/03/nia-to-open-regional-and-district-offices-by-june-2021/*

Jafaru, M. (2018). Ghana Card; those with no ID documents to register under oath. *Graphic*. *https://www.graphic.com.gh/news/general-news/ghana-card-those-with-no-id-documents-to-register-under-oath.html*

Nyabor, J. (2019). NIA charging foreigners $120 for non-citizen Ghana Card. *Citi Newsroom*. *https://citinewsroom.com/2019/07/nia-charging-foreigners-120-for-non-citizen-ghana-card/*

Kasapa FM Online (2021). Reports of ongoing mass registration false – NIA. *Ghanaweb*. *https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Reports-of-ongoing-mass-registration-false-NIA-1270444*

Mybeeponline (n.d.). Know the upgraded features of the Ghana Card. *https://mybeeponline.com/know-the-upgraded-features-of-the-ghana-card/*

NIA (n.d.). Our Vision as NIA. *https://nia.gov.gh/*

NIA/b (n.d.). Learn more about FIMS. *https://fims.org.gh/faq/*

Starr FM (2018). We are not accepting Voter ID card for Ghana Card – NIA reacts. *Ghanaweb*. *https://www.ghanaweb.com/GhanaHomePage/NewsArchive/We-are-not-accepting-Voter-ID-card-for-Ghana-Card-NIA-reacts-701829*

Starr FM (March 2020). We're also Ghanaians – Fulanis roar over Ghana card, passport discrimination. *Ghanaweb*. *https://www.ghanaweb.com/GhanaHomePage/NewsArchive/We-re-also-Ghanaians-Fulanis-roar-over-Ghana-card-passport-discrimination-888529*

Yeboah, C.N. (2021). Banks reject voters, national identification card for transactions. *MyJoyOnline*. *https://www.myjoyonline.com/banks-reject-voters-national-identification-card-for-transactions/*

Legislation:

Data Protection Act, Act 843 of 2012.

National Identification Authority Act, Act 707 of 2006.

National Identity Register Act, Act 750 of 2008.

National Identity Register Amendment Act, Act 950 of 2017.

National Identity Register Regulations, LI 2111 of 2012.

ANNEX 1

OVERVIEW OF EVALUATION FRAMEWORK

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

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

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

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

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

RULE OF LAW TESTS

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

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

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

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

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

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

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

RIGHTS-BASED TESTS

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

These tests ask five questions about:

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

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

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

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

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

RISK-BASED TESTS

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

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

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

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

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

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

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