Digital Identification and ICT-Driven Development in Africa

ICT India Working Paper #49

Nirupam Bajpai and John Biberman

May 2021

Center for Sustainable Development
EARTH INSTITUTE | COLUMBIA UNIVERSITY

Abstract

In recent years, countries across the African continent have begun implementing solutions based on Information and Communications Technology (ICT) for challenges ranging across the spectrum of sustainable development. The programs which have been implemented so far have produced impressive results, and in aggregate, they demonstrate the potential of a digital Africa which applies ICT to accelerate the improvement of human development outcomes in the pursuit of a more prosperous, equitable society. However, for these programs to live up to their full potential, they must be coupled with comprehensive, national digital identity systems. Digital identification not only boosts the efficiency of individual ICT-driven development initiatives, they permit seamless coordination between both public and private programs at all levels. While some African countries have established digital identity systems, but there is room for improvement in order to make them fully inclusive, transparent, and effective. In this, African governments can use India's Aadhaar digital identity system as a model for how to accomplish these objectives within the framework of a universal, highly integrated system, even under constraints of limited resources.

Introduction

For decades, Information and Communications Technology (ICT) has played an integral role in the diffusion and implementation of government services in developed and developing countries alike, with some of the most notable applications taking place in Africa. In past decades through the present day, ICT tools have been essential in spreading essential notifications and knowledge from the public sphere down to the popular sphere, whether through radio broadcasts, video productions, or SMS systems. The common factor in all of these applications was that technology was being used to disseminate information and services, from the top down, to ordinary citizens in a way which was vastly more efficient and widespread than prior, analog methods.

However, new technological advances have created the basis for a newly collaborative relationship between governments and citizens with the benefit of ICT. Digital platforms can allow citizens to take the initiative in receiving government services from education to healthcare online, while governments can target investments towards ever more granular segments of the population through the same advances. In agriculture, data about soil nutrition and crop quality, which would traditionally be gathered by sweeping networks of extension agents, can be collected via satellite or drone technology and relayed directly to farmers, with a digital link to expert advice should there be need for further consultation. In health, digitization of insurance and care infrastructure has allowed for an explosive increase in telemedicine, creating both primacy and specialist care opportunities where none existed before. Meanwhile, in education, ICT has allowed for individualized targeting of students according to needs and goals at a scale never before seen, while offering unprecedented flexibility for extended education. Most of these applications have occurred in the private, non-profit, or public-private partnership space so far, but fully integrating these advances into the provision of government services would revolutionize the relationship governments have with their citizens.

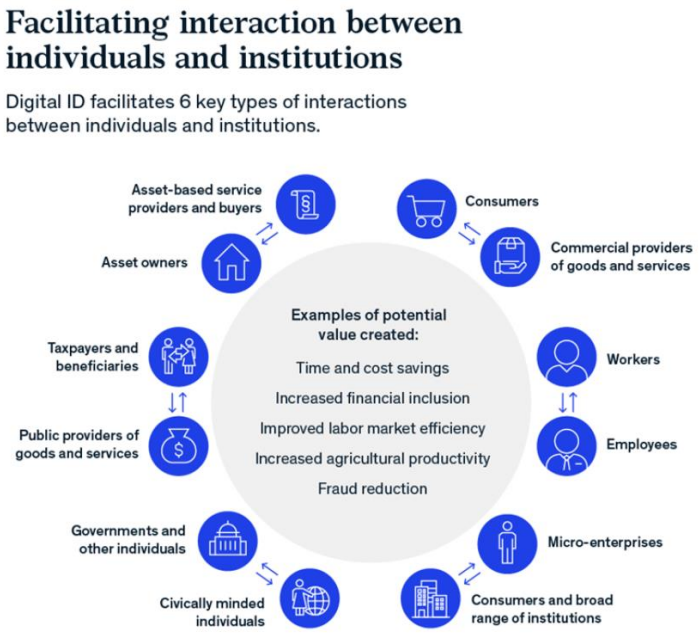
However, a robust and universal digital identification system is a mandatory prerequisite for the achievement of this public digital revolution. Digital ID provides more than a means of verification that an individual, removed by the distance that technology affords, is who they say they are. It is a means of cataloguing and organizing the needs and desires of these same individuals in a way that enables coordinated action at scale. With the additional support of government data, a digital ID can link together programs specific citizens would benefit from, allowing for government to take the initiative to deliver precise monetary and non-monetary support for these citizens. However, digital ID is the keystone to all the possibilities that these new technologies afford for delivering greater services on behalf of the government to the people. In the absence of digital ID, not only will many of these platforms not function optimally, many will fail to take shape altogether. Therefore, any government wishing to elevate its e-governance to the next level must first invest in developing a strong, flexible, and accommodating digital ID system which every one of its citizens will be able to use and benefit from, without inviting the risk that these same systems will further isolate citizens who are already disenfranchised.

Numerous African countries have already implemented their own digital ID systems in the pursuit of greater inclusion, growth, and government efficiency. Nigeria’s eID program, one of

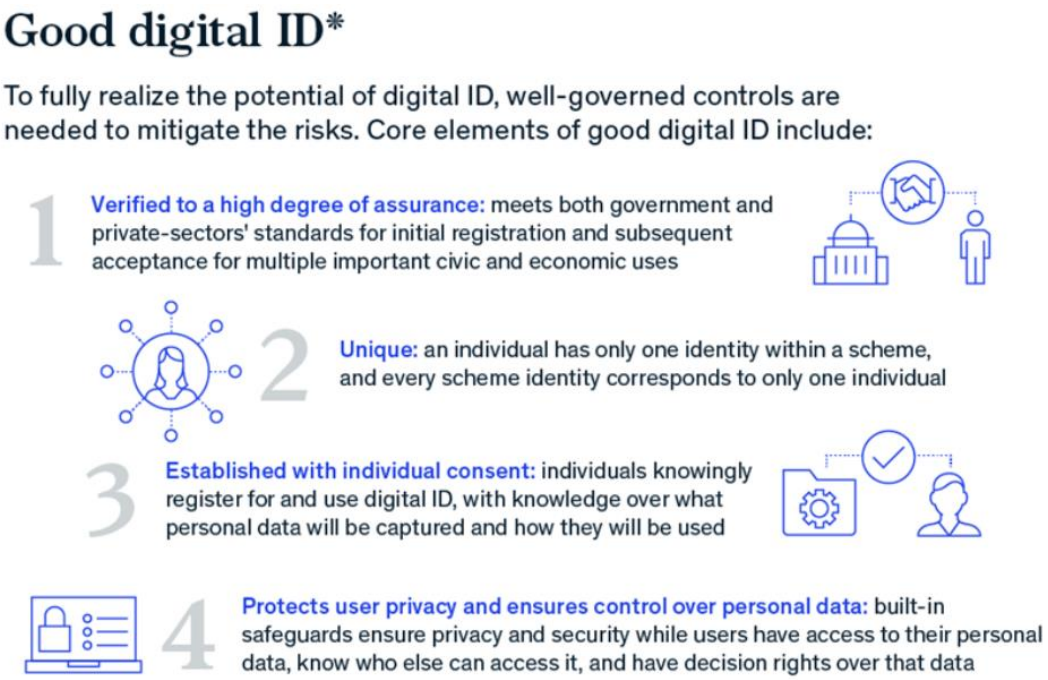
the most developed in the region, dates back to 2014, while Kenya's National Integrated Identity Management System (NIIMS), known otherwise as *Huduma Namba*, was launched in 2019. However, while the scope and ambition of these programs have been laudable, they have on occasion failed to reach some of the most excluded and vulnerable citizens, repeating the patterns of other types of government services. This has in some cases widened the digital divide, rather than narrowing it. For countries in the region to fully realize the promise that digital ID holds for their own development, they will need to implement global best practices for making these services universal, easily accessible, and a means for government and the population to frictionlessly interact with each other. India's Aadhaar program can serve as an excellent example of how governments can accomplish these goals in a similarly resource-constrained environment.

The Importance of Digital Identity

Digital identity, mentioned in Sustainable Development Goal 16, is a means to achieve economic, civic, and social empowerment across the spectrum of society. An effective digital identification program creates the basis for rapid transactions of all types, grounded in the trust that comes from the verification of one's identity. This facilitation of trust has remarkable social and economic benefits. A McKinsey Global Institute study found that implementing digital ID could increase GDP in emerging economies by as much as 4-13%, with these gains largely accruing to individuals. Over half of these gains would come from the most basic form of digital identification, a simple proof of identity, while the remainder would come from "advanced digital ID, which features the capacity to share data and link between databases using the digital ID as a foundation. The nonmonetary benefits of digital ID could hold even more potential; well-implemented digital ID could lead to safer internal and external migration, improved education and healthcare systems, more accessible labor markets, higher rates of civic participation, and stronger legal protections against trafficking and exploitation.



Applications and use cases of digital ID. Source: McKinsey Global Institute



The four characteristics of "good" digital ID. Source: McKinsey Global Institute

The most sophisticated digital IDs can provide a legal identity to those who lacked it before, of whom there are one billion across the entire world, and can provide digital functionality to the additional 3.4 billion who have legal ID, but have no ways of using it in the ICT space. This unlocks great potential for increasing inclusion in a number of ways. Digital ID will drive formalization, which increases the transparency of interactions while reducing fraud and making rights easier to enforce. Digitization itself will also make services more rapid, easier to use, and more fully streamlined with other platforms.

This raises the question of what constitutes a "good" digital ID. McKinsey identifies four pillars: first, the ID must feature verification and authentication to a standard that allows users to trust it for important applications. This can be accomplished via means across the spectrum of technology, such as biometrics, passwords, QR codes, or codes embedded in smart devices. Second, the ID must be unique, with a single number for each individual and a single individual corresponding to each number. Third, users must be able to use the ID in a manner of informed consent, registering for it voluntarily and knowing where and how their data is used. Finally, user privacy and control over personal data must be made a top priority, with users given access and control over their personal data, including decision rights over who is provided access and full transparency.

Ten Principles on Identification for Sustainable Development. Source: World Bank.

All types of ICT, on their own, are fairly neutral. They have the tendency to amplify a society's tendency towards a particular set of values, but what these values are must be determined by the framers of the technology themselves. This means that for all the potential benefits of digital IDs, they carry a particular set of risks too. For instance, they could facilitate the persecution and targeting of ethnic and religious groups. Unprotected personal data could be sold for profit, used to manipulate electoral results, or abused to impose social control via surveillance and restriction of key functionalities such as payments, travel, and social media access. Databases could be subject to security breaches, especially those maintained by partner institutions with less capacity than the central government. And finally, inclusion could be disrupted by technological problems with the hardware or software underlying the digital ID, interrupting use disproportionately in infrastructure-poor areas. To mitigate these risks, national digital ID initiatives following

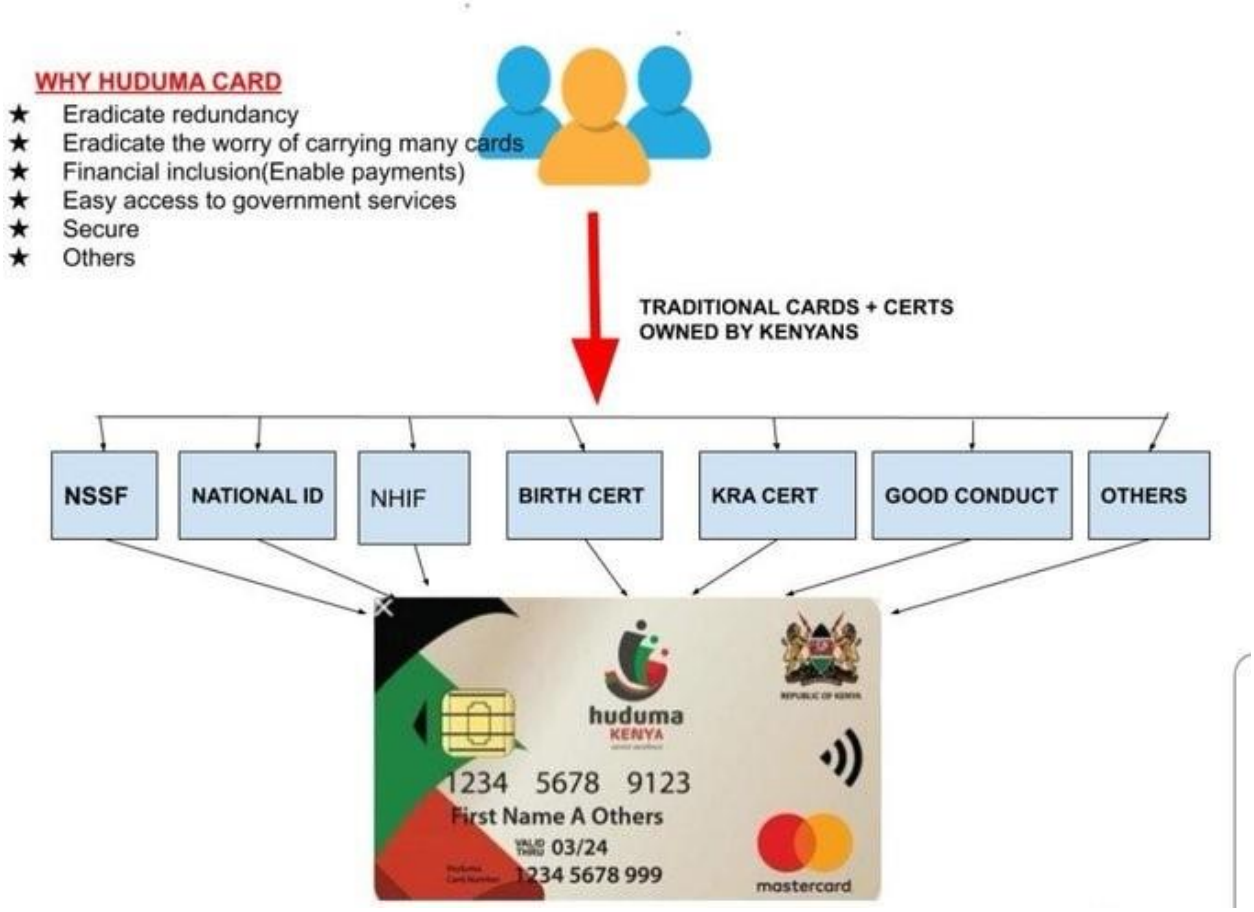
international best practices should focus on building privacy protection principles into every facet of their system, such as minimal, proportional data usage and retention. To push back against institutional manipulation and abuse of the digital registry by government agencies and associated figures, these programs should institutionalize processes for dealing with disputes which avoid arbitrary judgements and encourage adherence to the rule of law. A fuller accounting of the principles which allow digital identification to be in full compliance with the Sustainable Development Goals can be found in the above figure.

Case Study: NIIMS in Kenya

Kenya is currently in the process of implementing one of the most ambitious digital ID initiatives on the African continent, but it is not the first in the region to attempt to do so. That honor belongs to Nigeria, whose eID program, introduced in 2014, has attained substantial success over the past seven years. Initially conceived as a financial inclusion initiative, the eID can also serve as a national identity card, a travel document, and even a payment card. Registration for the eID requires only the collection of the applicant's National Identification Number (NIN) and biometric data in the form of fingerprints. As of May 2020, over 41 million Nigerians had registered for the eID, and future iterations of the program are planned for the implementation of applications for e-services in areas such as voter registration, health, and transport.[1] Since 2017, however, eID adoption has stalled due to challenges with public-private partnerships and difficulties integrating separate government identification systems together. Kenya's digital ID program is far more nascent, which makes its current state considerably more reflective of the challenges which other African governments seeking to realize the full e-governance potential of digital identification will face. It therefore merits a more in-depth examination.

The National Integrated Identity Management System (NIIMS), known otherwise as *Huduma Namba*, was announced in 2019, with the goal of creating a new, digitized version of Kenya's existing civil registry. Kenya had previously made prior attempts at implementing digital ID, such as the National Digital Registry System (NDRS), which was announced in 2014, then abandoned. *Huduma Namba*, however, features a far more sweeping potential scope than that program. In addition to creating portable and digital records of individual biographic and biometric info, the NIIMS database will link to other existing government databases, concerning areas such as land ownership, social welfare, and education. New personal information will also be collected on citizens and permanent residents registering in this new system, including nationality, birthplace, family relations, marital status, education and employment status, disability, agricultural activities, and fingerprints. This constitutes a level of individual personal data collection significantly beyond that of other peer digital ID programs.

[1] https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/nigeria-eid



Huduma Namba overview. Source: Amani National Congress Party.

The Government of Kenya describes *Huduma Namba* as an engine to lift people out of poverty by providing them with a means to verify their personal identity, pointing to how the initiative supports Kenyan President Uhuru Kenyatta's "Big 4" development agenda. First, NIIMS is intended to improve the affordable housing situation by generating data on the number of households and the number of occupants within each household for sharing with civil planners. Second, the program is intended to lay the groundwork for universal, affordable healthcare by connecting to the National Hospital Insurance Fund (NHIF) database, making information available for use by actors within the health sector, and by providing the means to identify patients accurately to ensure proper diagnosis and treatment while avoiding identity fraud and abuse. Third, data from the program will be used to boost the manufacturing sector by providing information on employment status and occupation, tied to biometrics, to economic planners. This information can be used to encourage labor market growth and increase foreign and domestic manufacturing investment. Finally, NIIMS should improve food security by contributing to a national database of farmers and farming households, allowing public resources to be deployed more efficiently.

These goals are not out of line with the goals of many other digital ID programs around the world. However, will the design of NIIMS actually contribute to their achievement? Conversely, would the program be capable of realizing unmentioned, more ambitious goals? A number of

fundamental flaws in the implementation of NIIMS are likely to limit its effectiveness, or even contribute to the digital divide. These are in the process of being addressed, but if they are not resolved, rather than contributing to social mobility and equality, this digital ID program could actually put access to public resources further out of reach for the most disadvantaged and vulnerable.

First and foremost, the NIIMS program has been designed to complement the existing civil registry, rather than to bring as many residents into the fold of legal recognition as possible. Registrants for *Huduma Namba* are required to present a substantial amount of personal information which they could only have obtained by previously registering in other government systems, such as a national ID number or a birth certificate. Simply put, when not everyone can prove their legal identity from birth, making proof of legal identity a registration requirement for a digital ID will make the new digital system off limits to the not insignificant share of the population with no such proof. The gaps in Kenya's civil registration system were consequential enough for the World Bank to issue an assessment in 2016 that the country's identification infrastructure was insufficient to support the vision of a national registration system. Unfortunately, under its current design, NIIMS will not aid in the solving of this problem.

A second challenge facing NIIMS is the lack of any meaningful data protection and privacy framework in Kenya. The National Data Protection Act (DPA) was passed in November 2019, but lacked many of the basic regulations for collecting, securing, accessing, and storing sensitive personal data which form the international standard. Nor has the law even been fully implemented – in fact, a number of key officers required by the DPA have not yet been appointed. Because this foundational requirement for gaining the public trust has not been met, the public has no way to determine whether the information accessed through the NIIMS database is secure or even accurate. While the core NIIMS ID system may not contain inaccuracies, the linked databases it relies upon frequently contain duplicate, conflicting, or even outright incorrect information, a flaw which cannot be addressed in an environment of security vulnerability and lack of transparency.

These concerns about lack of privacy and unequal access to legal identification are compounded by a history of discrimination in access to such documents, both circumstantial and intentional. For rural, remote, and pastoral communities, compiling any type of records has long been a barrier to increased legal security, due to challenges of distance, movement, and cost. In addition, the process of obtaining a physical ID card actually differs on the basis of ethnicity or religion, putting this crucial document out of reach for a number of minority groups. The fear, grounded in history, that unsecured sensitive personal data will be used to target further discrimination against these minority groups can only make them less likely to register for the program, even if they do have the required documents. By January 2020, the High Court had ruled that the NIIMS privacy and equality framework was not just inadequate, but in violation of the Right to Privacy enshrined in the Kenyan Constitution. The ruling mandated that a stronger framework be put in place before *Huduma Namba* could proceed, simultaneously banning the collection of any DNA or GPS data in connection with the program.

This would potentially be acceptable for an opt-in identification system, but the Kenyan government intends NIIMS registration to be mandatory to access all public services. Various

officials have issued different statements on this; a government spokesperson stated in March that the current national ID card would be phased out by December 12 this year to be replaced by NIIMS, contradicting an earlier statement by the ICT Cabinet secretary that the nationwide rollout of NIIMS would only begin in December 2021. If the government follows through with this goal, however, millions of Kenyans and permanent residents in Kenya who have had no prior means to register for their legal personal identity, and therefore have no means to obtain the *Huduma Namba* card, could be unjustly denied their right to access public services. An initiative which was likely originally conceived to be in service of the goal of development for the most vulnerable could ultimately create the opposite effect.

The chance to avoid waiting in interminably long lines to access government services was seen, not necessarily incorrectly, as a reason that Kenyans would jump to register for the new Digital ID system. However, due to the reasons stated above, the program has been plagued by low adoption rates, despite the looming effective mandate that all citizens and residents over 18 use the new ID scheme by the end of this year, along with a separate card for minors of at least six years of age. The program has attempted a number of strategies for increasing its registration rates, such as pushing SMS notifications to applicants who are eligible to collect their new cards. But by April 2021, only 10% of Kenyans had done so. In its overall approach to the program, the government has seemingly viewed digital ID not as a means to provide better access to resources for citizens and residents, but as a means of data collection and coordination for its own planning purposes. Amidst these barriers to registration and the lingering suspicion that personal information in the system would not be secure, the challenges encountered are unfortunately unsurprising.

Given these ongoing hurdles, the needs for *Huduma Namba* are clear. First, if this digital ID is truly intended to replace the existing national ID, this cannot be done in a vacuum. The legal documentation system will need to be reformed in that case to ensure that Kenyans genuinely do universally have the means to gain legal identification. This will be challenging in a short time, with many residents from remote and migrant communities lacking any existing concrete proof of their residency or citizenship. It is also an inevitable reform should the government wish to reach the goal of working for the benefit of all within its borders, whether a digital ID is involved or not. Since the challenges to registering every potential applicant in the short term are so great, and the stakes are so high, Kenya would likely benefit from a digital ID registration model similar to what India implemented through its Aadhaar program, described below. India has reached near-universal coverage with its cradle-to-grave digital ID system, despite similar challenges, by making registration requirements as minimal, quick, convenient, and painless as possible.

Second, Kenya will need to give its data privacy and protection framework enough teeth to create confidence in this novel, ambitious system. The existing system has been deemed inadequate by the country's own judicial system, and it lacks the personnel to be implemented even in its current form. The new data privacy framework will need to emphasize not just preventing outsiders from hacking into personal information, but also avoiding the accidental or intentional leaking of personal information from within the system. This will need to be balanced with a level of transparency surrounding linkages to Kenya's existing national databases in order to prevent codifying the data errors contained within these, which would further erode the public

trust. Ultimately, Kenya's new digital registry will likely need to be redesigned from the ground up, with universal access and data security as its foremost priorities.

Overcoming Resource Constraints in Digital Identity Systems: Lessons from India

India's Aadhaar system is frequently viewed as the gold standard in creating a universal, "cradle-to-grave" digital ID which meets both the needs and the resource constraints of developing countries. Introduced in 2009, Aadhar was first created to meet the need, encountered in so many other countries, for a single form of identification that would be universally accepted for public and private services. Today, 92% of the country is enrolled in Aadhar, and the system has over 250 programs connected to it. Aadhaar's implementation has by no means been perfect, but it offers a number of lessons which African countries can draw from in their quests to create their own digital IDs and realize this new potential for inclusion and growth.

First, like NIIMS, Aadhaar will likely become the ultimate proof of identity which Indians provide in order to access public and public-adjacent services. However, unlike NIIMS, Aadhaar has made inclusion of all types its utmost priority. The Aadhaar card is not linked to proof of citizenship, but rather, simple biometric identity. This means that for the first time, excluded and undocumented groups, often the most in need of government services, have been provided a means to access them. Provided that these applicants are introduced by an individual formally registered with the Unique Identification Authority of India (UIDAI), they can even apply without any other proof of citizenship or residency. This has served as a lone pathway to legal identity for millions across the country since the program was introduced. The "identity-first" model, as opposed to the "nationality-first" model, reduces barriers to providing basic identification for the populations which both lack it and need it most. By permitting linked applications to apply their own, stricter requirements for proof of nationality, the system also does not compromise on national security. An additional benefit of the "identity-first" model is the way in which its minimal data collection accelerates enrollment and reduces costs. Aadhaar now costs as little as 1.16 USD for a digital-only ID, making it accessible to even the poorest users. A similar approach to registering new cardholders would bear fruit in the African region, considering the similar financial and logistical challenges to obtaining a legal identity that poor and marginalized communities face.

Second, Aadhaar has provided worthwhile insights into the meaning of achieving inclusivity both in the enrollment process and at the actual point of service provision. For instance, ordinary biometric measures have proven unsuitable for blind Indians whose irises cannot be scanned, or for physical laborers whose fingerprints have been rendered illegible from the wear of their work. Special procedures have been developed to use alternative biometric measures for such groups. In the system itself, power and connectivity issues can lead to exclusion through a failure rate that is all too high. A 2017-18 study of the India Public Distribution System (PDS) found that Aadhaar experienced a failure rate between .8% and 2.2%. This points to the necessity of a conversation around the times and places where digital ID may not be appropriate. Government agencies may be highly interested in the potential for digital ID to combat fraud, but if it is deployed in an area with unreliable infrastructure, it could wind up harming access to public services on the whole.

Finally, India offers lessons in reckoning with the challenges of privacy and institutional trust created by digital ID systems. This is admittedly an area where Aadhaar has struggled. The Aadhaar repository continues to remain relatively unprotected, with several recent cases of fraudulent access and accidental leaks by partner agencies of personal demographic information. Even if the structure of Aadhaar authentication means that these personal details cannot be used to fraudulently obtain services, the information itself remains sensitive, and these incidents damaged public trust in a way which ultimately undermined the goals of the program. Both Aadhaar and the initiatives which follow its example should strive to maintain this trust by mainstreaming privacy into the design of their systems. Core principles to implement include limited data retention and collection, informed consent for data sharing, strong regulatory bodies for data usage, and institutional checks and balances for actors who violate these covenants of privacy. In this case, African governments can learn from Aadhaar's experience in order to create a system that is even more successful.

References

Desai, Vyjayanti T et al. "Ten Principles on Identification for Sustainable Development." World Bank Blogs, February 7, 2017. https://blogs.worldbank.org/digital-development/ten-principles-identification-sustainable-development

Huduma Namba. https://www.hudumanamba.go.ke

"Kenya's National Integrated Identity Management System." March 2020. Briefing Paper, Open Society Justice Initiative. Open Society Foundations, New York. https://www.good-id.org/en/articles/kenyas-national-integrated-identity-management-system-briefing-paper/

Kimuyu H., Nairobi News, 2021 https://nairobinews.nation.co.ke/editors-picks/expect-an-sms-if-you-registered-for-huduma-namba-ministry

Ramnath N.S. and Assisi C. *The Aadhaar Effect: Why the world's largest identity project matters*. 2018 Oxford University Press https://www.india.oup.com/product/the-aadhaar-effect-9780199487615

Sen S. "A Decade of Aadhaar: Lessons in Implementing a Foundational ID System", ORF Issue Brief No. 292, May 2019, Observer Research Foundation https://www.orfonline.org/research/a-decade-of-aadhaar-lessons-in-implementing-a-foundational-id-system-50464/#_ednref4

Thales Group. "Nigerian national ID program: an ambitious initiative." https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/nigeria-eid

Unique Identification Authority of India. https://uidai.gov.in/

White O., et al. "Digital Identification: A Key to Inclusive Growth." April 2019. McKinsey Global Institute. McKinsey & Company Available at https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth