Surveillance Enabling Identity Systems in Africa: Tracing the Fingerprints of Aadhaar

PRIVACY INTERNATIONAL

THE CENTRE FOR internet & society

AUTHORS:

Shruti Trikanad
Vrinda Bhandari

RESEARCH ASSISTANT:

Drupad U.

EDITORS:

Gurshabad Grover
Yesha Paul

Submitted to the Centre for Internet and Society
Edited by The Clean Copy | Layout Design by Indu Manohar

Table of Contents

Introduction

Following the 9/11 attacks, the global "war on terror" accelerated the deployment of identification technologies for the purposes of security, surveillance, and governance.[1] A range of identification and surveillance mechanisms were introduced by governments around the world, including new identity technologies for citizens, foreigners, and visitors alike, the use of biometrics at borders, and increased sharing of personal data between international actors.[2] Previous biometric identity proposals had often met stiff resistance from lawmakers and the public in the US,[3] but this radically changed post the attacks.[4] Even now, a range of governmental and intergovernmental bodies use biometrics to create watchlists, control movements across borders and access points, track and surveil people of interest, and perform forensic analyses.[5]

However, there has recently been a developmental turn in biometric identity, where the political justifications for implementing new policies have shifted from security and terrorism to promoting human development and enhancing social and economic inclusion,[6] particularly for the marginalised.[7] The Sustainable Development Goal (SDG) of "legal identity for all people worldwide"[8] has been transformed by several actors into the goal of establishing a "universal" or all-purpose legal identity that uses digital technologies and biometrics. The World Bank best embodies this, claiming that its Identification for Development (ID4D) initiative "uses global knowledge and expertise across sectors to help countries realise the transformational potential of digital identification systems."[9] In furtherance of this, the Bank has also supported the implementation and enhancement of many biometric identities and civil registration systems through its different projects, which will be discussed in further detail in this paper.

Simultaneously, a key motivating factor driving the push for introducing biometric identity programmes in developing countries is the popular narrative of the "success" of the Aadhaar identification programme in India. The Aadhaar model is characterised by a unique identification

number linked to an individual through their biometrics, which can then be used by them to access public and private services. The biometric and demographic data of the ID holders are stored in a centralised database managed by a public body (the Unique Identification Authority of India or UIDAI), which can be accessed by private and government service providers seeking to authenticate the identity of Aadhaar ID holders. In addition to these functionalities, a set of Application Programming Interfaces (APIs) has been built atop it to provide financial infrastructure for governments, businesses, start-ups, and developers.[10] The Aadhaar project promised all Indians formal identification that would better enable them to access welfare entitlements. The official purpose of the unique biometric identification system was to plug the leaks present in the welfare system in India, and "ensure that the fruits of welfare schemes reach the targeted population for whom such schemes are actually meant."[11] This was in response to claims that persons participating in welfare programs were fraudulently claiming more rations than they were eligible for, by using different identity documents. In its 2017–18 annual report, the UIDAI reported that the system had saved the government reduced "leakages" of INR 90,000 crores (or INR 900 billion).[12]

However, India's experience with Aadhaar for more than a decade has unearthed evidence of the consequent harms produced by national digital ID systems,[13] while evidence of the widely claimed benefits of these systems remains limited. Even the benefits claimed by the government, in the form of reduced leakages, have been disputed by researchers in India.[14] Issues such as exclusion from key services, discrimination, increased surveillance, and access to fundamental social rights have and continue to plague the Aadhaar system.[15] Additionally, the high costs involved in building and maintaining such systems give rise to questions on the reality of its benefits to citizens and governments. The amassing of big troves of data on citizens – nearly always accessible to governments with little to no control by the ID holders – has led to serious concerns of unchecked governmental power and risks of surveillance. It is important to note that even though these systems are designed to use citizen data only to govern the citizens' access to services, most of these ID systems are permitted by law to divulge key information to law enforcement bodies, courts, etc.[16]

In our report, we hope to identify the different external influences and actors that are playing a part in biometric ID programmes in developing countries. These range from philanthropic organisations, private companies, and technology vendors to state and international institutions. Our scope of research is limited to countries in Africa; as case studies, we are looking more closely at Nigeria and Kenya. During this exercise, it was also impossible to ignore another pattern: the new identification systems being built in these countries are all significantly similar in their design, application, and management, to the Aadhaar system. A key characteristic of the growing "digital identity for development" trend is the consolidation of different databases that record beneficiary data for different government programmes into one unified platform. This is ostensibly to increase convenience to consumers and create more efficient service delivery by government and private service providers. Additionally, to access these platforms, consumers can only use their unique ID with the help of biometric authenticators. Several other commonalities led us to explore in further detail if and how these developmental actors were promoting identity and social welfare systems that closely resemble Aadhaar.

Research Methodology

To research and write this report, we have primarily relied on four types of sources. For the first three we used desk-based research: First, we systematically examined reports from international organisations and key private and government players, while focusing on the World Bank; Second, we looked through the relevant provisions of the legal framework and case laws in India, Kenya, and Nigeria where applicable; Third, we used secondary resources such as news reports to supplement any gaps in our knowledge. Finally, we interviewed and spoke to various civil society organisations and academics with knowledge of the ID systems in Africa.

This research is focused on the African continent, specifically Kenya and Nigeria, to better understand the impact and influence of the Aadhaar narrative in these two countries. This required us to conduct an extensive literature review to identify the important actors in each country's digital ID ecosystem. We have attempted to investigate the links between the complex web of vendors, governments, NGOs, think tanks, philanthropic organisations, and supranational organisations like the World Bank that promote digital ID systems in multiple countries across Africa.

However, the funding and lobbying that drives policymaking are often deliberately obscured, making it difficult to directly connect certain actors with each other. We were further constrained by the difficulty in accessing important documents such as agreements between funders and recipients and contracts involving government and private players. This made it more difficult to ascertain the exact relationship between parties, and therefore, the nature of the influence exercised. It was particularly difficult to find all the policy documents of the countries we were studying – Kenya and Nigeria – that could have helped us determine the intention of the policymakers, and therefore, the influences at play. Thus, in some cases, there is no direct correlation, but important inferences can be drawn. Additionally, given our distance from the African continent and the language barriers (in terms of French, Swahili, and Yoruba), we may have missed certain local nuances that may have added crucial context to this conversation on digital IDs.

Despite these limitations, we hope this study provides an insight into the incentives and influences involved in the creation of a national ID system, as well as the roles of various private, governmental, and supranational actors that influence the development of national ID systems in Africa, specifically, Kenya and Nigeria.

The Aadhaar Ecosystem & the Actors Involved

In 2009, the Indian government passed an executive notification establishing the Unique Identification Authority of India (UIDAI), thereby putting in place mechanisms to build the world's largest centralised digital ID system.[17] In 2016, partly in response to constitutional challenges to the validity of the project, the government enacted the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 (the Aadhaar Act). Over time, the UIDAI was responsible for the enrolment of citizens using their demographic and biometric data (including the procurement process),[18] maintaining the authoritative source register, the Central Identities Data Repository (CIDR), issuing regulations regarding the administration of the Aadhaar project, and grievance redressal.[19]

1. Data Collected by UIDAI

As part of the Aadhaar enrolment process, the UIDAI collects demographic and biometric information. Every individual (excluding children below the age of five) must mandatorily provide demographic information regarding their name, date of birth, gender, and residential address – with the option of providing their email address and mobile number.

In cases of introducer-based enrolment, the UIDAI must additionally collect the introducer's name and Aadhaar number; while in the case of head-of-family–based enrolment, the name and Aadhaar number of the head of the family, one modality of their biometric information, and their relationship with the individual applying for an Aadhaar number are collected. Under the law, no information regarding race, religion, caste, tribe, ethnicity, language, records of entitlement, income, or medical history can be collected by the UIDAI.[20] The biometric information collected by the UIDAI comprises a photograph/facial image, all ten fingerprints, and scans of both irises (except for children below the age of five).

There are certain biometric exceptions provided so that residents who are unable to provide their fingerprints due to injury/deformity/amputation/other relevant reasons are allowed to provide only their iris scans. Additionally, the UIDAI is tasked with the handling of exceptions of individuals who are unable to provide any biometric information.[21]

Limited information is collected by the UIDAI for children below five years of age, such as their name, date of birth, gender, enrolment ID/Aadhaar number of any parent ("preferably" the mother), address of the child (same as that of the parent), the facial image of the child, and biometric information of one of the parents.[22]

2. The Actors in the Aadhaar Ecosystem

There are various actors in the Aadhaar ecosystem such as the registrars (approx 212), enrolment agencies (approx 755), requesting entities, biometric solution providers, authentication service agencies, etc.[23]

a. Registrars

Registrars are entities authorised by the UIDAI for the enrolment and verification of documents of individuals.[24] Registrars can be state agencies/departments, public sector undertakings – such as the Rural Development Department (for National Rural Employment Guarantee Scheme) or the Civil Supplies and Consumer Affairs Department (for TPDS), insurance companies such as Life Insurance Corporation and banks. Registrars either collect the biometric and demographic data of individuals directly or through enrolment agencies. Notably, registrars have the "flexibility" to collect additional data – termed "KYR+" or "Know Your Resident+". This includes data such as whether the individual is above or below the poverty line and their family details in cases where they avail of food subsidies under the Public Distribution System.[25]

The tasks of a registrar include, inter alia,

i. enrolment planning (comprising targeted enrolment numbers, locations, timelines, and reviewing/amending the list of Proof of Identity, Proof of Address, and Proof of Relationship documents);
ii. the selection and on-boarding of enrolment agencies;
iii. identifying and coordinating the establishment of the enrolment stations and enrolment centres;
iv. defining KYR+ fields and initiating technology integration for the data capture;
v. providing their public key to the UIDAI for encryption purposes; (f) finalising the process of data transfer to UIDAI;
vi. field-level execution, monitoring, and audit; and
vii. fulfilling their "fiduciary responsibility" and "duty of care" to secure and protect all the identity data collected from the resident.

The UIDAI also prescribes broad measures for data protection and security for them.[26] Registrars are appointed through MOUs or agreements for enrolment and are to abide by a code of conduct and processes, policies, and guidelines issued by the UIDAI.[27] Categories of persons eligible for appointment as registrars are limited by the Aadhaar (Enrolment and Update) Regulations, 2016.

b. Enrolment agencies

Enrolment Agencies are usually empanelled agencies that are hired by a registrar or the UIDAI, and assist in demographic and biometric data collection.[28] In turn, these agencies hire supervisors to manage and operate the enrolment centres. The UIDAI emphasises that "sub-contracting of Enrolment Work is not allowed for private/commercial Organisations/PSUs /Govt. Companies / Autonomous bodies. However, field-level manpower such as enrollment operators and supervisors can be hired through third parties." The details of the companies from whom manpower will be hired by the enrolment agency have to be disclosed in advance, although government entities have the option of franchising their enrolment work to CSCs/local government bodies.[29]

Enrolment agencies are given an enrolling agency code, using which the registrar can onboard such agencies to the Central Identities Data Repository (CIDR). The enrolment data is uploaded to the CIDR using certified equipment and software with the digital signature of the registrar/enrolling agency. The data is encrypted immediately upon capture. The decryption key lies solely with the UIDAI.[30]

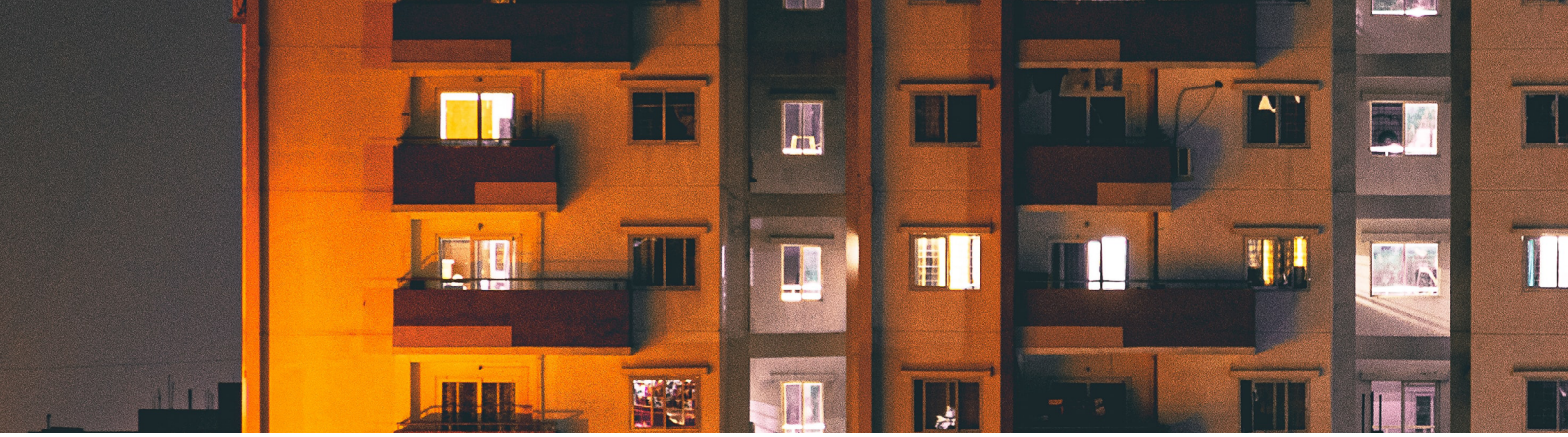
Registrars and enrolling agencies are obliged to use the software provided or authorised by the UIDAI for enrolment purposes. The standard software has security features as specified by the UIDAI. The registrars are prohibited from using the information collected for any purpose other than uploading it to the CIDR. Additionally, sub-contracting of the enrolment function is not allowed. The Code of Conduct also contains specific directions for following the confidentiality, privacy and security protocols, and submission of periodic reports of enrolment.[31]

c. Requesting entities (AUAs, KUAs, etc)

A requesting entity means an agency or a person that submits the Aadhaar number and demographic information or biometric information of an individual to the CIDR – which is a centralised database of all Aadhaar numbers issued to Aadhaar card holders – for matching.[32] The purpose of authentication or matching is to enable Aadhaar holders to prove their identity, and for service providers to confirm the resident's identity claim to provide services and access to benefits, consumer services, or subsidies.[33] The requesting entity sends a user's Aadhaar number and any other details needed for authentication to the Authentication Service Agency (ASA), which, in turn, sends it to the CIDR for authentication.

d. Authentication User Agency (AUA)

AUAs have been defined under the Aadhaar (Authentication) Regulations as "requesting entities" that use the "Yes/No" authentication facility provided by



the UIDAI. The Yes/No authentication facility is a type of authentication facility in which the identity information and Aadhaar number are matched against the data available in the CIDR, and the UIDAI responds with a digitally-signed response containing a "Yes" or "No", along with other technical details related to the authentication transaction, excluding identity information.[34]

e. e-KYC User Agency (KUA)

The other type of authentication facility is the e-KYC authentication facility, in which the biometric information and/or OTP and Aadhaar number securely submitted through a requesting entity are matched against the data available in the CIDR, and the UIDAI returns a digitally-signed response containing e-KYC data along with other technical details related to the authentication transaction. Therefore, a requesting entity that, in addition to being an AUA, uses the e-KYC authentication facility provided by UIDAI is called an "e-KYC User Agency" or "KUA".[35]

f. Authentication Service Agency (ASA)

Authentication only becomes available through an Authentication Service Agency (ASA), which is regulated by the Aadhaar (Authentication) Regulations, 2016, specifically, Regulation 19. ASAs are to use certified devices, equipment, or software duly registered with or approved or certified by an authority/agency. The systems and operations are audited by the Information System Auditor. The requesting entities pass the encrypted data to the CIDR through the ASA and the response (Yes/No authentication or e-KYC information) also takes the same route back. The server of the ASA must perform basic compliance and completeness checks on the authentication data packet before forwarding it to the CIDR.[36]
A list of ASAs uploaded by the UIDAI in August 2018 is available online and includes government companies such as Bharat Sanchar Nigam Ltd, private companies such as Mastercard India Services Pvt Ltd, private telecom service providers such as Bharti Airtel Ltd and Vodafone India Ltd and its group companies, and government agencies such as the Centre of e-Governance of the Government of Karnataka.[37] The requesting entities pass the encrypted data to the CIDR through the ASA and the response (Yes/No authentication or e-KYC) also takes the same route back.

3. The Role of Private Companies Involved in the Aadhaar Ecosystem

In the initial days of establishing the Aadhaar project, many tech/software companies such as HCL Infosystems, Accenture, and Wipro helped set up the Aadhaar infrastructure and carry out various functions such as biometric storage solutions, handling Aadhaar data and the UIDAI portal, deduplication, security systems, purchase of biometric authentication devices, and disk drives for the project.[38] Apart from iSpirit and MOSIP, which are discussed in this paper, there are other companies involved in the Aadhaar ecosystem, especially those that use the Aadhaar e-KYC option for "know your customer" requirements. The Securities and Exchange Board of India listed eight entities including the Bombay Stock Exchange and Central Depository Services (India) Ltd that were authorised to undertake Aadhaar e-KYC authentication after registering themselves as KYC User Agencies (KUAs). These eight companies had to allow the "SEBI registered intermediaries/mutual fund distributors to undertake Aadhaar Authentication in respect of their clients for the purpose of KYC."[39]

UIDAI has also entered into licensing agreements with foreign biometric solution providers. For instance, it executed a contract with L-1 Identity Solutions – an American defence contractor which provides the source code for biometric storage. The contract gives L-1 Identity Solutions access to all personal information about all residents in India. However, UIDAI retains sole ownership and the right to use all such data in perpetuity.[40]

In April 2019, based on a complaint by the UIDAI, the Telangana Police registered a criminal case against the Management of M/s IT Grids India Pvt Ltd and others.[41] The FIR was based on a complaint from an individual residing in Hyderabad, Telangana about the misuse and "illegal access and fraudulent use of sensitive identity information such as Aadhaar Number. Voter Identity details including colour photographs, beneficiary details of various Government Schemes and the data related to surveys conducted by the Government of Andhra Pradesh" by the company, M/s IT Grids India Pvt Ltd. The allegations against the company were that it was misusing the "Seva Mitra" application (that it had developed for the Telegu Desam Party) and stole voter information and Aadhaar data to engage in voter profiling, targeted campaigning, and even vote deletion.[42]

International Actors Influencing Identity Systems

Since the implementation of the Aadhaar system, similar ID and welfare projects have been encouraged around the world. For instance, officials from Afghanistan, Bangladesh, and Tanzania visited India to discuss the Aadhaar project. UIDAI's first head and India's former telecom regulator, R. S. Sharma, has also reportedly stated that countries such as Algeria, Russia, Morocco, and Tunisia have displayed an interest in understanding Aadhaar.[43]

This global interest is not always incidental. A range of international actors – both, public sector and private – have played a significant role in promoting Aadhaar and the idea of a foundational digital ID around the world. The international mainstream narrative has also presented a completely flattering view of Aadhaar, with The Economist noting that it has "streamlined the delivery of services and payments, cut corruption, boosted financial inclusion and hugely raised participation in India's digital economy," thereby "inspiring" many countries in Asia and Africa.[44]

This section identifies various international actors that have varying degrees of influence on digital ID systems being rolled out across the world, specifically in Africa.

1. World Bank

The World Bank has been one of the most prominent actors in pushing Aadhaar to countries across Africa and Asia. It launched the ID4D ("Identification for Development") programme in 2014, pursuant to which countries such as Morocco, the Philippines, and Myanmar came to New Delhi to learn more about the concept of Aadhaar and digital ID.[45] According to the World Bank, digital IDs are one of the four major enablers of digital development that will help achieve the SDG of providing legal identity for all by 2030.[46] The World Bank has consistently cited the importance of digital ID, specifically Aadhaar, as a tool for financial inclusion (especially amongst the unbanked population) and for efficient management of social programmes and welfare distribution by reducing wastage in welfare subsidy.[47]

In its 2016 Development Report, the Bank identified Aadhaar as an example of "transformational" technology, noting that digital identification systems such as Aadhaar, "by overcoming complex information problems, helps willing governments to promote the inclusion of disadvantaged groups."[48]

Paul Romer, the chief economist at the World Bank, has also reportedly wholeheartedly endorsed Aadhaar, stating:

> "The (Aadhaar) system in India is the most sophisticated (ID system) that I've seen. It's the basis for all kinds of connections that involve things like financial transactions. It could be good for the world if this became widely adopted. ...Other countries are also looking at similar programs, but research shows it's best to develop one standardized system so people can carry their IDs wherever they go in the world.[49]

The Bank views the Aadhaar Act as an example of a legal framework providing in-built efforts to ensure inclusion in registration, since Section 5 of the Act calls for the UIDAI to take special measures to issue Aadhaar numbers to women, children, senior citizens, persons with disability, unskilled and unorganised workers, and nomadic tribes.[50] It has further cited some of the measures taken by the UIDAI to improve security and oversight over the Aadhaar infrastructure.[51]

However, the World Bank's endorsements underplay the problems with exclusions and security concerns that have plagued Aadhaar in India.[52] Under the Indian system, individuals must undergo Aadhaar-based biometric authentication or furnish proof of possession of an Aadhaar number in order to access government welfare, subsidies, and benefits.[53] There have been multiple reports about ration cards (necessary to access food subsidies) being cancelled for not having been linked to an Aadhaar ID, leading to people missing out on their monthly food rations, and in extreme (and rare) cases, to death.[54] This was coupled with reports of indignity and hardship associated with obtaining food subsidies and benefits.[55] As per the State of the Aadhaar Report of 2019, 1.5% of the surveyed respondents who were accessing food rations (under the Public Distribution System) experienced a biometric authentication failure and were unable to receive their food rations in the previous attempt.[56] In addition, there have been various incidents and reports of unauthorised leakages of Aadhaar data from various government websites and through other third-party leaks and databases.[57]

It also misstates the contextual reality. For instance, the 2016 World Bank Report states that the Aadhaar programme in India had "dispensed with the physical ID card altogether."[58] However, this does not reflect the reality, wherein most individuals have a physical Aadhaar card that is popularly used and accepted as identity proof throughout the country, even though the law does not recognise the idea of an Aadhaar "card."[59]

2. World Economic Forum

The idea of a digital ID or a foundation ID has also been pushed at the highest levels at the World Economic Forum (WEF) at Davos. For instance, in 2018, the WEF released a report titled "Identity in a Digital World: A new chapter in the social contract" that discusses elements of user-centric "good" digital IDs.[60] The report cites Aadhaar as an example of an inclusive, centralised ID system, wherein the government had successfully enrolled 99% of its population with a unique ID by "making enrolment easy". This number seems higher than other estimates,[61] although, undoubtedly, the reach and scale of Aadhaar in India are near-universal. The report also acknowledged that "ongoing legal deliberations and policy making" in India were attempting to adequately balance the benefits of Aadhaar with the protection of fundamental rights.[62]

In 2019 –at a session on "Identity in a digital world" at the WEF Annual Meeting –the architect behind Aadhaar, Nandan Nilekani, said that Aadhaar was not a surveillance or data-gathering system, has been instrumental in ensuring welfare benefits were correctly targeted, and that issues with Aadhaar have been successfully "resolved".[63]

In 2021, the WEF published another report titled "Digital Identity Ecosystems: Unlocking New Value" as an interactive guide for executives focused on the methods of improving the digital ID ecosystem, especially in a post-Covid world.[64] The report, which featured the Government of India and Omidyar Network as contributors, praised Aadhaar for aiding in financial inclusion and reducing KYC costs by 86%, without noting any of the concerns around privacy, surveillance, or exclusion from social welfare programmes.[65]

3. ID4Africa

ID4Africa is an NGO movement that works with various African countries on their path to developing "robust and responsible identity ecosystems".[66] As part of its mission, ID4Africa has hosted conferences and meetings themed around "Identity Ecosystems for Service Delivery" and "Digital Public Goods Initiatives as Pathways to Identity Development".[67] As part of its work, ID4Africa collaborates with various private sector actors such as MOSIP and the World Bank; in that context, the narrative around the benefits of digital ID systems using the Indian example of Aadhaar has become popular. This helps influence policy development concerning several African countries.

For instance, at the 5th Annual ID4Africa Meeting 2019, Rajesh Bansal, the Regional Director of BFA Global and ex-UIDAI and IndiaStack Architect made a presentation titled "The Promise and Challenges of Inclusive Fintech in Developing Economies."[68] The presentation cited the Aadhaar ecosystem as an example of the importance of building digital ecosystems, describing Aadhaar as:

> built on an open platform and allows other organizations to create connected services. These layers of connected services have formed what is known as the "India Stack," which provides a digital infrastructure that facilitates presence-less, paperless, and cashless service delivery from anywhere in India.[69]

The presentation exclusively highlighted the benefits of Aadhaar and India Stack, such as facilitating e-KYC, sending direct payments to bank accounts (through Aadhaar Payments Bridge), transferring money via mobile (Unified Payment Interface), and sharing documents such as bank statements and utility bills with service providers that need to authenticate an individual's identity through DigiLocker.[70] The uncritical appraisal of Aadhaar is surprising, given the voluminous literature that exists around privacy, surveillance, and exclusions concerns surrounding Aadhaar-enabled infrastructure.[71] Further, the presentation simply accepted and endorsed the Indian government's claims made in 2018 of an estimated fiscal gain of more than USD 12.7 billion (around INR 98,533 crores) since 2013 from Aadhaar-enabled direct benefit transfers, without acknowledging the existence of various studies questioning such estimates.[72] Given that the audience for the presentations at the ID4Africa meeting included government representatives from across the world, the narrative of Aadhaar as a sole public good is further strengthened.

At the same ID4Africa meeting, Anit Mukherjee from the Center for Global Development, Washington DC, made a presentation titled "ID and Service Delivery: Emerging Evidence and Lessons from India", which heavily relied upon and praised the Aadhaar model in India.[73] The presentation cited Aadhaar as an example of digital service delivery that had been integral to the gains made in financial inclusion, including the linking of bank accounts with Aadhaar numbers. There was no discussion around the privacy concerns arising from digital IDs such as Aadhaar. It also elaborated on the role played by Aadhaar in improving the transfer of benefits and fiscal savings (of between 33%–35%)[74] through Aadhaar-enabled programmes such as PAHAL (direct benefit transfer of LPG cooking gas through one-time linking of Aadhaar, bank account, and mobile number), pension (direct benefit transfer to the bank account through Aadhaar-based deduplication and periodic authentication), and Public Distribution System (for monthly food rations through Aadhaar authentication at the point of sale).

While the presentation recognised the problem/possibility of failure of Aadhaar-based authentication and recommended human backup, it did not detail the extent of authentication failure. The Centre for Global Development concluded that 2% of the surveyed respondents had, on some occasion, not received their pension at all – either because multiple authentication attempts had failed or that 80% would ask the village revenue officer to withdraw. However, the sample size of this surveyed population is not mentioned in the presentation (nor is the underlying study cited).

These presentations evidence an uncritical endorsement of the use of big data for real-time governance, without any mention of surveillance concerns or the need for data protection laws and protocols. For instance, Anit Mukherjee's presentation cited the Andhra Pradesh Real Time Governance model, which builds on "real time data from Aadhaar authentications and digital transactions" and uses "integrated fingerprint, iris and face recognition hardware".[75] There is substantial literature that exists on the dangers of using facial recognition software and building on Aadhaar data,[76] but it does not seem like these concerns are being presented to the African countries and partners invited to these presentations organised by ID4Africa.

4. Private Players and Technology Vendors

Another undeniable influence in the biometric identification space in Africa is technology vendors and service providers. In the continent, the market for biometric and digital identity documents alone is estimated at €1.4 billion (or USD 1.46 billion).[77] This market is currently populated by a few major international players – powered by their financial, technical, and political capital.[78] While typically driven by profit motives, some of these companies are also connected to their governments in ways that complicates their intentions, as was speculated in the case of Civipol, detailed below.

a. Thales

Partially owned by the French Government, Thales provides defense, security, digital identity, and aerospace services.[79] In their own words,

> "Thales delivers identity and biometric solutions to governments, public authorities and private entities in the fields of civil identity and public security. We do this by providing highly secure documents such as passports, ID cards, drivers' licenses etc. that are at the heart of identity schemes.[80]

Currently, Thales is present within the biometric identity systems of Algeria, Cameroon, Nigeria, and South Africa directly. In Nigeria, it is acting as a supplier for Nigeria's new multi-purpose eID card.[81] Perhaps more critical, however, is its investments in other similar groups, resulting in the Thales group assuming an important role in ID systems across the continent. In 2019, Thales bought Gemalto, based in the Netherlands. Gemalto formed one of Thales' seven global divisions, to be named Digital Identity and Security (DIS).[82] This was reportedly motivated by Thales' intention of controlling the entire decision chain involved in digital security:

> "This combination creates a world-class leader with an unrivalled portfolio of digital identity and security solutions based on technologies such as biometry, data protection, and, more broadly, cybersecurity. Thales will thus provide a

seamless response to customers, including critical infrastructure providers such as banks, telecom operators, government agencies, utilities and other industries as they step up to the challenges of identifying people and objects and keeping data secure.[83]

b. Gemalto

Gemalto is an international digital security company, providing software applications and secure personal devices such as smart cards and tokens. It provides services for the Nigerian ID system through a subsidiary, Trub, and recently got a tender for the biometric identity system in the Democratic Republic of Congo.[84] Similar to Thales, in a move positioned toward being able to provide complete end-to-end solutions, Gemalto took over Cogent – 3M's Identity Management business – in 2016, thereby bringing all these companies under the umbrella of the Thales group.[85] In its 2018 activity report, Gemalto indicated that its "Identity, Internet of Things and Cybersecurity" business is benefiting from the growing number of government programmes relating to civil status registers and electoral records, having already shown 11% growth.[86]

c. IDEMIA

IDEMIA, another French company, was born in 2017 from the merger of the biometric entities of Safran, Morpho, and Oberthur Technologies. It specialises in biometric identification and security, as well as secure payments, with the aim of converging technologies developed for the public sector and those for the private sector. IDEMIA has its presence in several African countries, but most notably it is responsible for – and is managing – the biometric database in the Nigerian ID system (through Safran Identity and Security).[87] IDEMIA also found itself in some controversy recently, when it was awarded the tender to provide biometric kits for the Huduma Namba system in Kenya. It was reportedly unclear how they were awarded the tender and was soon banned when found to be illegally conducting business in Kenya since it did not have local offices as required by the Kenya Companies Act (2015).[88] During Kenya's 2017 election, IDEMIA denied accusations of misconduct and claims of its biometric voter identification system being hacked,[89] even in the presence of concerning reports that showed that voter data was available for sale in the run-up to the election.[90]

d. IN-Groupe

IN-Groupe is a French private limited company that offers identity solutions and secure digital services and is partly owned by the French state. Between 2019 and 2020, it acquired Surys – an identity document authentication company, and Nexus – a software company that creates automated processes to manage the

full lifecycle of both physical and digital identities.[91] IN-Groupe is developing the biometric ID platform for the Republic of Djibouti,[92] Mozambique, and was recently selected to help design and secure a new digital identity scheme for the Principality of Monaco.[93]

Other companies operational in African countries include Mühlbauer (German), active in the biometric ID systems of Uganda and Mozambique;[94] and Veridos (German), active in Zambia, Uganda, Morocco,[95] etc.[96]

Apart from their hold on the market, these companies have also been actively engaged in advocacy that encourages the "digital identity for development" agenda on the continent, particularly through their memberships in groups, as will be demonstrated further.

e. Security Identity Alliance (SIA)

Established as a global non-profit, the Secure Identity Alliance "brings together public, private and non-government organizations to foster international collaboration, shape policy and provide guidance on the key issues of legal identity."[97] Their mission, as expressed on their website, is to "help shape global identity policy addressing the key issues throughout the identity journey– from enrolment and issuance to use case development and implementation."[98]

SIA was founded by Thales and IDEMIA, and has, as members, other familiar names such as IN-Groupe and Veridos. Recently, Philippe Barreau, the VP of IDEMIA, and Didier Trutt, the CEO of IN-Groupe, were elected as Chairman and Vice-Chairman of the board, respectively, to lead the trusted identity advocacy programme.[99] SIA has published literature on and hosted/co-hosted several events aimed at promoting the use of digital identity for social inclusion and economic development in Africa.[100] Several of these were in collaboration with the World Bank and the ID4Africa initiative.[101] SIA's Open API Initiative or OSIA has been particularly ubiquitous in the continent. OSIA is a set of APIs developed by SIA that provides a simple, open standards–based connectivity layer between all key components and systems within the identity ecosystem.[102] The initiative encourages countries and technology partners to download the functional and technical specifications and implement them in their customised ID systems, and for governments to reference the API as 'open standards' in their tenders.[103]

OSIA has also been heavily advertised by ID4Africa as a solution to the vendor lock-in problem that many ID projects in Africa have suffered from.[104]

f. MOSIP

MOSIP is a modular and open-source identity platform, run by the International Institute of Information Technology in Bangalore, India. It forms the basis on which national foundational IDs are built. Its stated aim is to help "user organisations such as Governments implement a digital, foundational ID in a cost-effective way, while embracing the best practices of scalability, security and privacy" by harnessing the power of open source.[105] It advertises its services for the government under the head "MOSIP for Governments" to help "enable" the country's "foundational identity system to be its own strategic asset."[106]

MOSIP is aimed at enabling robust digital identities across the world, and, so far, has over 59.5 million people registered on MOSIP-based systems.[107] Its model is perhaps best explained through the following screenshot from its website:[108] In the private sector, MOSIP – which is funded by the Bill & Melinda Gates Foundation, the Omidyar Network, TATA Trusts, and NORAD (the Norwegian Agency for Development Cooperation)[109] – has played an important and influential role in pushing the idea of foundational digital ID across Asia and Africa. Replicating the Aadhaar model, with its surrounding APIs, i.e. "India Stack" is difficult. Hence, MOSIP has emerged as the open-source modular platform for helping countries establish a foundational ID programme.[110]

As The Economist describes it, MOSIP has set out "to give countries with far less IT capacity than India's a basis for establishing a cost-effective foundational identity system that was, in effect, 'Aadhaar in a box'."[111] It is, thus, perhaps unsurprising that MOSIP has the support and endorsement of Nandan Nilekani, the architect responsible for Aadhaar in India.[112] Bill Gates has gone on record referencing MOSIP when talking about the important role played by the private sector in facilitating financial inclusion and has used India as an example of plugging leakages (presumably through Aadhaar).
In an interview with CNBC TV 18, he stated:

> The role of the Gates Foundation as an advocate for those who don't have access to financial inclusion, is to make sure that there is technology and standards, including open source work that we are providing through the financial switch which is called Mojaloop and through the digital identity system (…) called MOSIP.[113]

Since its foundation in 2018, MOSIP has been actively involved in working with governments across Asia and Africa in building their digital ID systems. Reportedly by 2023, the aim is to have at least 10 countries operating MOSIP-based digital-ID platforms, moving it closer to an international standard.[114]

Most recently, in November 2021, it signed an MoU with the Togolese Republic towards establishing its foundational digital ID system for the identification and authentication of all persons in the country. MOSIP partnered with the national agency, ANID, to aid with technology transfer, capacity building, and technical support in the adoption of the platform.[115]

In addition to its work with Togo, MOSIP is already working with the Kingdom of Morocco and the Republic of the Philippines to support the establishment of their digital ID systems, providing support in the transfer of code, documentation and knowledge, platform adoption, and capacity building.[116] MOSIP completed a pilot successfully in the Republic of Guinea and is currently working with the governments in Ethiopia and Sri Lanka on the implementation of their pilots.[117] In some countries such as Ethiopia, this work is taking place simultaneously with efforts to draft a national data privacy law.[118]

For its work across the African continent, MOSIP has worked closely with ID4Africa. In 2019, the South African government organised the 5th Annual ID4Africa Meeting in Johannesburg on the theme "Identity Ecosystems for Service Delivery". More than 1500 participants attended the meeting, including representatives from 50 African countries and national identity authorities and users, international development and humanitarian agencies, civil society members, solution providers, and domain experts. MOSIP also participated in this meeting, met various government representatives, and even made a presentation on its approach to foundational identity in the session titled "Disruptive Innovations".[119] In December 2020, MOSIP participated in ID4Africa's livecast on "Digital Public Goods Initiatives as Pathways to Identity Development", which featured a discussion on how to hasten the value and realisation of digital foundational ID systems through multiple players.[120]Finally, MOSIP also presented its vision of digital identity at an event organised in conjunction with the UN General Assembly.[121]

The influence of Aadhaar in the roll-out of MOSIP can also be illustrated through MOSIP's team. The Chairperson of the Technology Committee is Sanjay Jain, who was the Chief Product Manager at the UIDAI (the body responsible for

the roll-out of Aadhaar) and a volunteer with iSPIRT, the Indian Software Product Industry Roundtable. Other members of MOSIP's executive committee such as Sanjay Anandram and Sharad Sharma are theAmbassador and Co-founder of iSPIRT, respectively.[122] It has also been reported that Bangalore was selected as the city to host MOSIP to enable them to draw on the "technical know how from Mr. Nilekani's original Aadhaar team" as well as the iSPIRT volunteers and resources in Bangalore.[123]

g. Civipol

Civipol is a French company that builds cooperative internal security projects with states and is the technical cooperation operator of the French Ministry of the Interior. In total, 40% of it is owned by the French state, and further, it is part-owned by large arms producers, including Thales, Airbus DS, and Safran. Financed almost exclusively by international sponsors, CIVIPOL has a presence in over 80 countries.[124] Currently, it is involved in identity systems in Senegal, Côte D'Ivoire, Central African Republic, Mali, and the Democratic Republic of Congo.[125] Apart from offering identity services, they also offer services for controlling cross-border migration, modernising interior security services, capacity-building for personnel in interior security, reinforcing local and regional migration policies, and strengthening and supporting anti-terrorist efforts, among others.[126]

Civipol is deeply connected to the French state: Prefect Jounot Yann, a former National Intelligence Coordinator, has been the chairman and chief executive of Civipol since June 2017,[127] along with Pierre de Bousquet de Florian, who was appointed chief of staff for Interior Minister, Gérald Darmanin, and served as the national intelligence coordinator as his predecessor.

In Senegal, they provided technical assistance in a project funded by the European Union's Emergency Trust Fund for Africa ("EU Emergency Trust Fund") to strengthen their civil registration system and link it to a biometric database.[128] The EU Emergency Trust Fund was founded in 2015 for "stability and addressing root causes of irregular migration and displaced persons in Africa."[129] Similarly, in Mali, in another project funded by the EU Emergency Trust Fund, CIVIPOL, along with the Belgian company, Enabel, is working to strengthen and modernise their civil registration system and link it to a biometric database.[130] Their presence in Côte d'Ivoire[131] and the Central African Republic[132] to modernise and expand their civil registration systems is also funded by the European Union. These projects, as described on their website, align with their mission to ensure a reliable and secure identity for all citizens as a basic right.[133]

However, a report released by Privacy International in 2020 showed that the funding by the EU Emergency Trust Fund, particularly to finance the biometric technology systems in Senegal and the Ivory Coast, was likely intended to help identify undocumented citizens in Europe and aid their return.[134] They report that the Côte d'Ivoire biometric identity system project description explicitly states that it is to be

used to assist in the identification of Ivorians irregularly residing in Europe and to organise their return more easily.[135] The goal of creating a biometric database, they claim, is that once a person is identified by immigration enforcement agencies in Europe and their biometric data collected, it can be compared with the data in the African systems, allowing them to be fast-tracked back to their home country.[136]

Among documents in this project disclosed to Privacy International[137] is one that repeatedly highlights the need to ensure that any biometric collection will take into account the data of the Senegalese living abroad.[138] It is also very likely that the recipient country accepting returning immigrants was a possible condition for the funds allocated by the EU.[139]

This effort by the EU and CIVIPOL that potentially mixes contradictory goals of development and surveillance is another reason to be wary of external influences on national digital identification programmes.

Case Study: Kenya

In Kenya, conversations around digital ID are situated among concerns regarding citizenship documentation, legal identity, and concerns of statelessness, especially among Kenyan border communities, minority groups, and non-white immigrants.[140]

The African Union Commission released its "Digital Transformation Strategy (DTS) for Africa (2020-2030)" which viewed digital ID, "particular[ly] using biometrics", as an important tool to support the digital economy and ecosystem. The strategy focuses on the economic and social benefits of digital ID, its role in supporting and facilitating the African Continental Free Trade Area (AfCFTA), and its importance in furthering human rights. The strategy identifies data privacy breaches, cyber-attacks, and cyber fraud as areas that may undermine trust in the digital economy. Therefore, it recommends that countries establish legal and regulatory frameworks that protect privacy, security, and user rights, and ensure that their digital ID systems are inclusive, privacy-friendly, secure, interoperable, and built using open standards.[141]

1. World Bank Welfare Programmes

The World Bank and its associated organisations have had a more complex (and less transparent) role in Kenyan identity systems. Through several of its programmes, it incentivised the creation of different civil registries, enhanced their coverage, and merged or centralised existing databases.

In 2016, the Bank (under the ID4D initiative) released its assessment of the Kenyan identity ecosystem. At the time, it was analysing the various identity systems that co-existed in Kenya, along with its Integrated Population Registration System (IPRS), which sought to allow select actors to conduct verification checks on identity documents.[142] In this document, the Bank claimed its broad objective was to better understand the nature and capabilities of Kenya's ID system, its role in development in the country, and how best to work with the country to strengthen this.

This assessment was also from the perspective of the identification needs of the Government of Kenya's "operational engagements";[143] presumably, this refers to the other collaborations that the Government of Kenya has with the World Bank. The Bank has been supporting several developmental programmes in Kenya, which have been influential in the design of the identification systems in the country.

The National Safety Net Program for Results (NSNP) started in 2013. It was meant to support Kenya's efforts to target safety programmes for poor and vulnerable households.[144] Mainly, it sought to integrate five of Kenya's main cash-transfer programmes by establishing a coordinated framework: the Cash Transfers to Orphans and Vulnerable Children (CT-OVC), the Hunger Safety Net Programme (HSNP), the Older Persons Cash Transfer (OPCT), the Persons with Severe Disability Cash Transfer (PWSD-CT), and the Urban Food Subsidy Cash Transfer (UFS-CT).

Among other things, the Bank sought to strengthen programme systems that ensure good governance, for cash transfer programs. In its appraisal of this project, the Bank recommended that the five programmes adopt common standards based on the emerging best practices in the sector, which include:

i. strengthening the programme to ensure that only those households that are eligible for the programme are selected;
ii. establishing a single registry to strengthen the checks on enrolment, thereby providing additional confirmation that households registered in the programmes are eligible for support;
iii. adopting internal controls on the payrolls produced through the programmes' electronic Management Information Systems to ensure that the correct amount is paid to beneficiaries;
iv. contracting payment service providers that make payments electronically and use two-factor authentication to ensure that payments reach the intended beneficiary efficiently and effectively.[145]

It identified the existing targeting and verification procedures to be limited in their ability to use existing data in corroborating household eligibility for programme support, and, therefore, have limited application to minimise leakage in the system. Through this project, the Bank hoped to (i) strengthen the verification of beneficiary eligibility by adopting a single registry to share information on beneficiaries among the five programmes and with the civil registration system, and (ii) improve the internal controls on the programme payrolls.[146]

In 2021, the Bank released an Implementation Completion Report, where they reported that the single registry of beneficiaries (across all five programmes) that they supported was operational and successfully provides a consolidated source of information on the cash transfer programmes, permitting cross-checking and reconciliation.[147] Along with this registry, they put in place a technology-based payment system that allows beneficiaries to receive payments under a two-factor

authorisation procedure.[148] Similarly, the Bank intervened in the Cash Transfers for Orphans and Vulnerable Children through a loan of USD 126 million[149] The objective of this programme was to increase social safety-net access for extremely poor OVC households and to build the capacity of the government to more effectively deliver the National Safety Net Programme. Among activities included in this programme was to "expand biometric enrolment for the program beneficiaries to facilitate payment authentication and pilot alternative payment mechanisms."[150]

In its implementation completion and results report, the Bank reported that a firm was engaged to conduct biometric enrolment for beneficiaries, along with which an electronic payment mechanism with two-factor authentication was also instituted.[151] This, they reported, greatly improved the Government of Kenya's capacity to implement the National Safety Net Programme initiatives, and made cash transfers more "secure, accessible, and predictable".[152] They also attributed to the project the successful strengthening of the integrity of management systems, the improvement of targeting mechanisms, and the consolidation of financial management processes.[153]

In a simultaneous project in 2018, the Bank opened a link of credit with the Government of Kenya in the amount of USD 250 million with the objective of "strengthening delivery systems for enhanced access to social and economic inclusion services".[154] This project is built on the success of its previous NSNP project that established the single registry – a database of NSNP cash transfer beneficiaries linked to the Integrated Population Registry System (IPRS) – and instituted a two-factor authentication payment system.

Here, the Bank aims to enhance the scope and coverage of this single registry by adding a social registry module. This new module would register households that can be identified as potential beneficiaries for SP programmes and will continue to establish a link to the IPRS for verification of data against Kenya's civil registration databases.[155] This would harmonise registration countrywide and offer readily available data on the country's poor and vulnerable population, which can reduce targeting and registration costs.[156]

In 2019, the World Bank approved a USD 750 million International Development Association (IDA) credit to achieve the Kenyan government's Vision 2030 objective. Part of this support is targeted towards the agricultural sector for reforms supported by the Kenya Inclusive Growth and Fiscal Management Development Policy Financing facility for better targeting of agricultural subsidies. The aim is to improve targeting through biometric digital identification and e-vouchers, such that the agricultural inputs reach the intended beneficiaries more efficiently.

As per the World Bank's press release:

> "By supporting the advancement of digitization through the creation of the national digital ID and pushing for access of internet services to all Kenyans, the facility will enhance service delivery by the government to its citizens, and reduce the need for face-to-face interactions and corruption opportunities.[157]

The Inclusive Growth and Fiscal Management development programme has, as one of its goals, to "leverage digitization to support the government's inclusive growth agenda."[158] The Bank's credit and the accompanying press release reflect its focus on achieving good governance through the use of digital technology.[159]

In the Financing Agreement for Credit,[160] the Government of Kenya is mandated to "enact, through its Parliament, amendments to the Registration of Persons Act to establish a National Integrated Identity Management System, with the mandate to assign a unique national (digital) identification number to all registered persons".[161]

The project appraisal document explains this mandate a little further through the benefits it sees with the unique biometric ID – particularly for the targeting of subsidies, social protection programmes, and e-medical services, among others.[162]

However, the Bank recognises the concerns with making digital IDs mandatory or even de facto mandatory, i.e., when the digital ID is legally voluntary, but in practice, is required to access important services or make important transactions. As per the World Bank, a "strict conditioning of essential government services on the presentation of a specific ID can be problematic if access to that ID system is not universal or is applied in discriminatory ways."[163] In fact, both India and Kenya have faced legal challenges that have raised concerns about the mandatory/de facto mandatory nature of their digital IDs.[164]

2. National Integrated Identity Management System

In 2005, the Kenyan government began the process of harmonising systems of registration of persons through the Integrated Population Registration System (IPRIS).

Thereafter, in 2018, the government passed the Executive Order No. 1 of 2018, which established the National Integrated Identity Management System (NIIMS), intended to provide a single ID and a "single source of truth" and personal information for all Kenyans and foreigners residing in Kenya and to provide access to national identification data.[165] Thereafter, the government passed the Statute Law (Miscellaneous Amendments) Act, 2018, which amended various provisions of existing statutes, including the Registration of Persons Act (Cap 107 of the Laws of Kenya) (RP Act). The amendments to the RP Act provided a statutory basis for the establishment of a national population register through NIIMS.

Thus, NIIMS is the national programme intended to establish an integrated biometric population database that "will be the 'single source of truth' on persons' identity data."[166]

To populate the NIIMS database, Kenyan citizens and foreign residents had to provide their sensitive personal data, including biometrics, to establish, verify, and authenticate their identity. In turn, they received a unique identification number called a "Huduma Namba" or Kenya's third-generation ID card.[167]

The Kenyan government has identified various benefits of NIIMS including national development, planning for equitable resource allocation, and de-duplication that will result in significant savings.[168]

As part of its function, NIIMS is intended to create and operate a national population register as the "single" source of personal data of all Kenyan citizens and residents; to assign a unique national ID number to every registered individual, to verify and authenticate identity information, and to harmonise and incorporate information from other government databases to the NIIMS register.[169] The intended benefits are improvement in national security, addressing de-deduplication, and creating a national reference frame for the provision of services (such as cash transfers and health services).

Challenges identified by the Kenyan government include a lack of documents, network issues, existence of many manual labourers, and the fact that there will be opposition to the project in the beginning, although, "eventually most people will come onboard."[170] Some of these concerns were litigated before the Kenyan High Court by the Nubian Rights Forum, the Kenyan Human Rights Commission, and the Kenyan National Commission on Human Rights. Among other features, the petitioners herein challenged: (a) the requirement to have a primary identification document to register for NIIMS; (b) the collection of DNA and GPS coordinates to register for NIIMS; (c) the mandatory enrolment for access to welfare services and the ensuing exclusion and discrimination; and (d) the procedure for passing the amendment.

During the hearing of the case, Kenya enacted the Data Protection Act, 2019, which was also considered by the High Court. In January 2020, the High Court found that the collection of DNA and GPS coordinates was intrusive and unnecessary and that it lacked specific statutory authorisation, and was, hence, unconstitutional. The Kenyan government was permitted to proceed with the implementation of NIIMS and process and utilise the NIIMS data on the condition that an "appropriate and comprehensive regulatory framework" for its implementation is enacted in compliance with the Constitution.[171]Consequently, the Kenyan government notified two subsidiary laws – commonly referred to as "Huduma Regulations"[172] – to create a statutory basis for data collection and to establish NIIMS as the main source of identity.

Thereafter, in October 2021, the High Court issued a further judgement on judicial review that held that the roll-out of Huduma Namba was illegal because the government had failed to conduct a data protection impact assessment in accordance with Section 31 of the Data Protection Act, 2019 (which was held to apply retrospectively). The court directed the government to conduct such a data protection impact assessment in accordance with the act and the Data Protection (Civil Registration) Regulations, 2020 before processing any further data or rolling out the Huduma Namba cards.[173]

The NIIMS system has been compared by scholars to the British kipande system, in terms of the latter's requirement of fingerprinting adult male Africans (who had to carry their identification documents at all times around their neck), the resistance put up by the people, and the identity card's facilitation of "reputation management".[174] Some of the risks identified by the Open Society Justice Initiative for NIIMS reflect concerns raised in the Indian example relating to privacy, intentional or accidental disclosure/leak of sensitive personal data, and high risk of error and exclusion.[175]

3. Influence of Aadhaar: Policy Narratives and Statutory Similarities

The influence of Aadhaar and the Indian digital ID experience is palpable in Kenya and on the operation and design of NIIMS. Apart from the general roles played by various international and private actors in promoting digital ID across Africa using the experience of India, there are specific instances of the Aadhaar narrative influencing the Kenyan journey as well. In fact, in its briefing note on NIIMS, the Open Society Justice Initiative (which provided legal support to plaintiffs challenging the way NIIMS was introduced) observed that "India's Aadhaar system is consistently cited as a model for centralized identification systems that provide a 'unique number from cradle to grave.'" [176]

This is perhaps best exemplified by the World Bank's ID4D 2016 Country Diagnostic Report for Kenya, published before the 2018 amendments to the RP Act were enacted and NIIMS was established. The report mentioned the Indian experience with Aadhaar as an example that could be considered by Kenya for its e-ID system, going as far as to state that "It could be useful to plan a visit to India and Pakistan by a group from Kenya that combines representatives from both the ID providers and ID users."[177] The report makes various recommendations for Kenya to strengthen its functioning identity system, citing the example of India.

The report of the World Bank and its endorsement of Aadhaar in 2016 seems to have had an impact, as is evident from the establishment of NIIMS and the roll-out of the Huduma Namba in 2018. A perusal of the amendments to the RP Act in 2018 revealed that many of the Bank's recommendations were implicitly accepted.

Further, in 2019, the Kenyan Ministry of Information and Communication Technology released a Digital Economy Blueprint to provide a conceptual framework for developing and growing the Kenyan digital economy.[178] The blueprint highlights the importance of a dynamic policy and legal framework, which includes "demonstrating digital leadership." It provides examples of countries that are at the forefront of such digital leadership by issuing digital IDs and adopting digital financial infrastructure to allow their citizens to become digital citizens. Among the examples cited by the Kenyan Ministry is that of the Indian government, which "has issued more than 1 billion 12-digit "Aadhaar" identity numbers to the country's residents."[179]

a. Architecture

Both the Aadhaar and NIIMS are centralised digital ID systems that rely on the collection of biometric data. Section 9A(2) of the RP Act provides the basis for such a centralised system by laying out the functions of NIIMS, including (a) creating and operating a national population register as a single source of personal information on all Kenyan citizens and residents; (b) assigning a unique national ID number to all registered persons; (c) harmonising and collating all the information relating to the registration persons in government databases into NIIMS; and (d)centralised printing and distribution of the national IDs.

In their challenge to NIIMS before the Kenyan High Court, the petitioners brought an Indian cyber security expert, Anand Venkatanarayanan, to testify as PW-2. Based on a review of documents, he deposed on various aspects of NIIMS:

> "The first was that NIIMS is functionally and architecturally similar to the Indian Aadhaar system. His second conclusion, based on the first, was that it would result in the same outcome, namely an endeavour which would pose a massive risk to personal security and privacy of the Kenyan residents with no demonstrable benefits. Lastly, that it would also create national security risks to Kenya, which would be impossible to mitigate.[180]

The rationale behind his arguments regarding the functional and architectural similarity of NIIMS and Aadhaar was that both (a) are centralised systems; (b) proceed on the false assumption that the use of biometrics eliminates the possibility of duplication since they can be used as unique identifiers; and that (c) the identification of a person by a human being is more accurate than identification by a machine or algorithm.[181]

Incidentally, both Aadhaar and NIIMS rely on private sector involvement. After the Supreme Court of India effectively struck down Section 57 of the Aadhaar Act for enabling "commercial exploitation" of personal data by private actors, the Indian government passed the Aadhaar (and Other Laws) Amendment

Act, 2019, which established a voluntary authentication mechanism for use by private entities.[182] In Kenya, the RP Act and the Huduma Namba Regulations are noticeably silent on the private sector use of the NIIMS database, which raises concerns about their access to the NIIMS database or identity data.[183]

However, an important source of variance between Aadhaar and NIIMS is the legal primacy of the digital ID. In India, Aadhaar is not considered a single source of information. Except for access to welfare services and payment of taxes,[184] Aadhaar cannot be sought in preference over other ID documents.[185] In Kenya, however, this primacy seems to be extended to all services. Under the Huduma Namba regulations, NIIMS is statutorily given preference as the primary means of identification for any government agency.[186]

b. Unique Number at Birth

In its 2016 Diagnostic Report, the World Bank recommended having a unique number from birth, which would also strengthen the birth registration process in Kenya – which faced issues of duplication of information, lack of interoperability, and clear integration "between birth/civil registration and the national identity issued to all the citizens."[187] To achieve this, the national ID would have to be issued at a younger age to decrease the time between birth and registration, which, in turn, would increase the "integrity" of the registration process. At that point, Kenya's National Registration and Identification Bill provided for the registration of children between 12–17 years of age.

The World Bank used the example of India, where the Aadhaar programme "is registering children as young as 5 years old" by collecting their fingerprints and iris data.[188] In India, Aadhaar numbers can be issued to children soon after they are born, although fingerprint and iris scans will only be collected once they turn five years old. Children must update their biometrics (i.e., fingerprint, iris scans, and photographs) once they turn 5 years old and 15 years old; although, at age 18, they can revoke their consent for the issuance of the Aadhaar number.[189] Interestingly, while one of the stated benefits of Aadhaar for children is tracking lost children,[190] newspaper reports have emerged documenting the misuse of Aadhaar and manipulation of demographic data (such as age and date of birth) to facilitate human trafficking.[191]

In 2020, the Kenyan government began the process of fresh identity enrolments, requiring individuals to provide existing identity documents. During the enrolment exercise, they also enrolled children, reportedly using their birth certificates and social security documents and taking their photographs.[192] The exercise of such governmental power was challenged before the High Court in the NIIMS case.[193]

c. Data Collection

The influence of Aadhaar on NIIMS can also be traced in the manner in which both digital ID systems have been conceptualised and operationalised and the importance of the recommendations of the World Bank.

In Kenya, the colonial Kipande system that was subsequently integrated within Kenya's RP Act, 1947 required an individual to disclose their ethnicity and clan. Based on the controversy surrounding this, including its (mis)use for political mobilisation, the government amended the act in 2018 and eliminated the prerequisite for disclosing ethnicity.[194] This is similar to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 where the UIDAI can collect the name, date of birth, and address of an individual, but is prohibited from collecting any information about an individual's race, religion, caste, tribe, ethnicity, language, records of entitlement, income, or medical history.[195]

Similarly, in its report, the Bank noted that iris scans have"successfully" been used in India's ID system and that the associated costs and benefits must be evaluated before it is introduced in Kenya.[196] Thereafter, the 2018 amendment to the RP Act increased the amount of biometric data collected. Apart from the fingerprints and photographs that were traditionally collected, the amendment prescribed the collection of retina and iris patterns (as in India), hand geometry, earlobe geometry, voice waves, DNA in a digital form, and GPS coordinates of the individuals' addresses.[197] As stated earlier, the collection of DNA and GPS coordinates was halted by the Kenyan High Court.

d. Verification and Authentication of Persons

The World Bank, in its diagnostic report, also recommended that the Kenyan ID system verify people in addition to verifying documents, since, at the time of its publication in 2016, the Automated Fingerprint Identification System (AFIS) operated by the National Registration Bureau in Kenya did not offer individual authentication. The AFIS could not handle requests from other users of identity services to authenticate persons based on their digital prints. The system could verify the credentials of individuals (by verifying their documents) but could not authenticate their identities (by authenticating their biometrics).[198]

Thus, while biometric data in terms of photographs and fingerprints were being collected during registration, it was not being used to identify and authenticate individuals. This was resulting in the creation of various independent biometric systems, such as for certain social transfer programmes, for use by the Independent Electoral and Boundaries Commission, and proposed use by the Pensions Department.[199]

According to the World Bank, as the ID system moved towards remote application, it would become imperative to facilitate individual identification and avoid the proliferation of public programmes that capture biometrics using incompatible systems. In this context, the report stated that a programme similar to Aadhaar

> "would enable the central database to provide a simple yes/no response to authentication queries from border posts, financial institutions, pension programs and other authorized users.[200]

After the 2018 amendment to the RP Act, the Kenyan government tasked NIIMS with the function of "verify[ing] and authenticat[ing] information relating to the registration and identification of persons."[201] Thus, under the current system, much like in India, individuals must get their ID documents validated and their identity biometrically authenticated. Similarly, the Huduma Namba regulations authorise the linking of civil registries and public agencies with the NIIMS database to facilitate authentication.[202]

e. Enrolment and Linking to Welfare Services: Concerns of Exclusion and Discrimination

Like Aadhaar, there were concerns of exclusion and discrimination in the case of the roll-out of Huduma Namba, especially for those persons and communities (such as the Nubians and other nomadic, pastoral communities) who did not have underlying primary ID documents. Additionally, the vetting procedures for the national ID for minority communities were more stringent.[203] Even of the 2.2 million people who registered for the cards, only 300,000 responded to texts about cards, leaving many cards uncollected.[204] This had a significant impact, considering the government's proposal for the mandatory linking of Huduma Namba with access to certain government and private services.

Before the Kenyan High Court in the NIIMS case, the petitioners' Indian expert, Anand Venkatanarayanan, cited the Aadhaar experience to depose that, as the size of the database grows larger, the enrolment rejection rate of individuals would increase. This would exclude people at the enrolment stage itself.[205]

He cited a paper published on the Indian government's use of Aadhaar for biometric identification, which found that, out of India's population of approximately 1.2 billion, around 10 million people (0.8% of the population) would be excluded from the Aadhaar infrastructure due to a false positive biometric match.[206] He similarly relied on the evidence emerging from India's Aadhaar experience to testify that the reliance on biometrics for authentication would result in the exclusion of certain marginalised sections of the population.

The Kenyan High Court acknowledged the concerns of discrimination and exclusion – both, in the sphere of enrolment and biometric authentication for access to welfare services – but it did not find that to be a sufficient reason to declare NIIMS unconstitutional. However, the "adequate and comprehensive" legal and regulatory framework that was directed to be implemented by the government was required to address the possibility of exclusion from NIIMS and the potential for discrimination.[207]

f. Technology Procurement

The World Bank report cited the Indian experience (of using open, standards-based procurement) when it came to technology procurement to reduce cost and improve competition amongst vendors, stating that "Kenya, like India, should move to a 'plug and play' system."

Developing nations in Asia and Africa have been impacted by the harmful misuse of data where data was created, reused, and repurposed for ill-intentioned purposes.[208] The Bank emphasised that countries expanding their e-government options, specifically digital identification systems, need to lower the barriers to digital adoption. The report also suggests e-procurement options in countries like India for other countries to draw inspiration from. This could "improve the quality of infrastructure", and as mentioned earlier, promote competition with the "winning bidder likely to be from outside project regions".[209]

Countries in Africa were already automating the digital processes related to specific government functions.[210] Much like the early days of UIDAI being attached to the Planning Commission in India, Kenya's national ID system is regulated by the National Registration Bureau. The NRB is a part of the Ministry of Interior and Coordination of the national government. Controversies have surrounded the software licensing of the NIIMS database without adequate safeguards for international third-party clients.[211] Furthermore, in 2019, a tender for biometric operations was awarded to IDEMIA, shrouded with legitimacy concerns for illegal business activities.[212] It is also pertinent to note that IPRS was established and integrated across systems by another foreign company with a lack of data protection policies to clarify how the data was collected, stored, and utilised.[213]

Case Study: Nigeria

In their Africa Business Plan report, the World Bank identifies four (among many other) "regional trends" in identification systems in Africa that warrant redressal[214]:

1. Limited coverage and accessibility have been achieved by the existing identity/CRV programmes.
2. The fragmented management (and governance structure) of current systems, with different ministries taking charge of different functional (and in some cases, foundational ID systems).
3. The lack of utilisation of technology in the CRV systems; most population registries and identity systems still operated largely by registering people and facilitating transactions using paper-based processes.
4. The systems were not able to achieve interoperability among themselves, allowing for disconnected functional systems operating simultaneously that were not able to interact with the CRVS.

This focus on interoperable identity systems that use technology to offer services is observed through much of the Bank's activities, particularly in its role in the Nigerian identity system.

In 2020, the World Bank, through the International Development Association (IDA), authorised a credit of USD 115 million to the government of the Federal Republic of Nigeria (FGN) for the development of its digital identification system.[215] The goals that the Bank and the Nigerian government (FGN) articulated in this agreement, as well as in the stipulations that the Bank put on the FGN about the structure of the ID programme, reflect the Bank's definition of the ideal digital system for a country like Nigeria.

This model is strikingly similar to that of Aadhaar, which, according to the popular narrative, is very successful in addressing the issues prevalent in developing countries.[216]

1. History of Nigerian Identification Programmes

Identification systems in Nigeria have taken many forms over the years. In 1978, the Department of National Civil Registration (DNCR) was set up within the Federal Ministry of Interior (FMI). DNCR was tasked with enrolling every Nigerian citizen 18 years or older and issuing a national identity card based on biographic data. This programme failed in 18 months. In 2001, the DNCR restarted their identification programme, intending to issue identity cards based on barcode technology. This project used a private service provider, Sagem, but was quickly shelved in 2006 after allegations of impropriety over the award of the bid to the firm.[217] The contracted firm had completed enrolment of 52.6 million out of 60 million residents and issued 37.3 million identity cards before closing operations.[218] It cost the FGN roughly USD 236.8 million. Amid this, in 2006, the DNCR set up the Harmonisation Committee to advise on the harmonisation of different identification systems in the country.

2. Final Report of the Committee on Harmonisation of National Identity Cards, 2006

The intention behind the setting up of this committee was "to review existing ID card projects and recommend ways of integrating them into a single multi-application card."[219]A multi-application smart card was the recommended way forward.

> "The Committee found that the global trend is a gradual move from a single purpose card to a more secure multi-application smart card. Accordingly, the Committee recommends the creation of a new National Identity Database, which will serve as a central source of identity verification. The Database will be connected to existing databases that are relevant to the identification of citizens and residents. The connectivity between the various databases, government departments and law enforcement agencies will be enhanced by the use of chip-based General Multipurpose Card (GMPC) technology, which allows for input of several applications on one card.[220]

Since Nigeria already had several databases that recorded identification information, the system the committee recommended for a foundational identity was to be built atop the existing structure. A central hub termed the "super-structure" would carry out validation of data and would be connected to the other components that comprise the GMPC system.

Other functions of the super-structure include access control of the whole GMPC project, setting standards (interface, business rules, etc), and controlling workflow.

Service centres (SC) will be linked to the super-structure and have their own equipment to carry out the registration of applicants and issuance of GMPCs.[221]

The super-structure would also be connected to legacy systems, the existing databases that are hosted by government agencies. The legacy systems will be responsible for capturing all details, i.e., biodata, biometrics, photographs, and other details specific to the agencies' statutory responsibilities. The legacy systems will interact with the super-structure for inquiries and update functions in respect of GMPC holders. The legacy systems will also maintain fingerprint data according to their requirements, based on agreed-upon world standards.[222]

The legal sub-committee, in turn, made the following recommendations:[223]

1. Removal of credit status information: Although it envisioned that the identity card may, in the future, be upgraded to be a smart card that has payment functionalities, it believed that – as per the Constitution – financial transactions are private and therefore information on the credit status of an individual should not be in the public domain. Access to such information must be specifically allowed by the owner of the information.

2. The legal sub-committee was of the view that all Nigerian security agencies should be able to access all the information in the national identity card for purposes of identification. Respective government agencies should be permitted access to information relevant to their mandate.

3. Access to the identity database should be restricted and only granted to relevant government agencies as provided by law. The committee also considered the ownership of the databank (and therefore, the data) to reside with the government and as a national critical information infrastructure that must be protected by law and technology. Any access by individuals should be specifically granted by relevant government agencies and provided for by law.

4. It also recommended the addition of other biometrics to be collected from citizens including genome sequence, blood type, etc.

In 2020, this report was updated, and a major shift that occurred was that the committee recommended making the NIN mandatory for use by all government departments. It also suggested that SIM network providers mandatorily link the NIN to issue SIM cards.[224]

This was prompted by the United States' denial of visas to Nigerians because of inadequate information and fears of terrorism.[225] The development also demonstrates how the goal for a centralised digital identity starts from "development" and quickly switches to "security" when needed.

The role of the World Bank in harmonising the different systems and placing the NIN as the foundational identity platform for Nigeria is not small. On its website charting its engagement with different countries, the Bank states,

> The World Bank is providing financial support by catalysing a total investment of $430 mln, which includes co-financing of $100 mln by Agence Français de Développement and $215 mln from European Investment Bank. The World Bank is also offering complementary technical assistance (TA) to reform the digital ID and civil registration ecosystem. The TA delivered so far included support for the development of a Strategic ID Roadmap endorsed by the highest levels of government (the Federal Executive Council), end user research focused on gender barriers to accessing identification, and national consultations with key marginalised groups (e.g., persons with disabilities) to receive feedback on the proposed project design and their barriers to accessing identification.[226]

In 2015, the Bank released its Nigeria Diagnostic report, which assessed the existing Nigerian digital ID situation, and recommended how a strategic roadmap could be created to address its gaps. This included, among others, the following recommendations:[227]

1. Scale-up the identity system, with speed.
2. Mobilise resources and support partnerships: The federal government should prioritise mobilising sufficient resources for identity development in Nigeria and may consider fiscal appropriations, donor contributions, and private sector participation.
3. Sharpen the vision of identification with an emphasis on rapid scale-up, full integration, and cost optimisation.

In 2016, the FGN – led by NIMC with support from the World Bank – held a high-level policy workshop on identification in Abuja, Nigeria. The workshop highlighted the role of digitally enabled identity in Nigeria's economic and social development as well as possible options and steps to developing identification in Nigeria. During April–June 2017, the FGN and the World Bank held consultations in Abuja with government agencies and stakeholders involved in identification in Nigeria. The strategic roadmap has benefited from the studies and consultations and has been funded by the ID4D programme of the World Bank.[228]

Importantly, the Bank recommended that the FGN set a time period to achieve its identification goals, one that is surprisingly short for such an ambitious project. It advised that the objective of universal coverage of a unique, official identity for every person in the country be achieved within 3–5 years.[229] It also emphasised linking the foundational system with other agencies including security services, the private sector, and ECOWAS.

While security agencies, including the defence, immigration, police, and prisons, require a way to verify the ID of a person, the private sector including banks, telecommunications service providers, and health centres require authentication services. The roadmap also recommended that Nigeria's digital identification programme be linked with regional use of ID, currently being undertaken by ECOWAS to promote cross-border free movement of people, regional trade and commerce, and a regional digital economy.

The ecosystem approach, another feature considered a "success" in the Aadhaar system, was recommended to alleviate the cost of setting up the system.

> "Partnerships may lower the cost, alleviate capacity, and promote sustainability of the program: Developing a modern, robust identification program is a gargantuan undertaking for a government. The development can pose a fiscal burden on the FGN, capacity constraints on the government's limited technical capacity, and risks on the longer-term sustainability of the program. The FGN may leverage partnerships, with government agencies, ecosystem players, and the private sector, to expedite the development and lower the cost of the program.[230]

3. The World Bank's Digital Identification for Development Project

In 2020, the World Bank released its Nigeria Digital Identification for Development Project that aims to "increase the number of persons with a national ID number in a foundational digital ID system", co-financed through an IDA credit of USD 115 million, USD 100 million from the French Development Agency, and USD 215 million from the European Investment Bank.[231] Two key documents in this project, IDA's Project Appraisal Document on a Proposed Credit[232] and the Financing Agreement,[233] ("the Agreements") shed some light on the influence these organisations are exerting on the FGN's vision for its national identity programme.

a. The Success of the Aadhaar Foundational System in Achieving Developmental Goals and Inclusivity

Claiming that the lack of accessible identity is a key factor behind the poverty, inequality, youth unemployment, and gender inequality in Nigeria – the World Bank suggests the implementation of a strong foundational ID system to ensure economic development, security, governance, and efficient delivery of services. Drawing on the experiences of other countries, it suggests that the foundational ID system serve as a platform upon which both the public and private sectors can rely for downstream transactions and service delivery. The model that reflects "good practices" from countries such as India and Peru is clear: digital identification systems that can uniquely identify registrants and are closely

linked to civil registration; is interoperable with sectoral systems (for instance, social protection, health, education, financial services, and so on); and does not connote legal status.[234] These, the Agreements add, can quickly scale to achieve full coverage and become a valuable tool for effective service delivery and poverty reduction. This emphasis is also clear on the purpose of the project that introduces us to the report:

> "Nigeria Digital Identification for Development Project will support the National Identity Management Commission to increase the number of persons who have a national identification number (NIN) reaching about 150 million in the next three years. This will enable people in Nigeria, especially marginalised groups, to access welfare-enhancing services.

The Bank's reliance on the Aadhaar model for solving problems of inaccessibility common to developing countries is also evident from its collaboration with the Unique Identification Authority of India (UIDAI) – the body managing the Aadhaar system – to gain knowledge and expertise regarding the Aadhaar system. In an article in the Economic Times, the UIDAI claims it is sharing the "broad framework and architecture of the Aadhaar project, the enrolment and authentication strategy followed by us and the update process" with foreign countries that intend to replicate the same.[235] Nigeria was reportedly the first country to send a team to India under the aegis of the World Bank to study the UIDAI model.[236]

b. A Unique Foundational Digital Id, with Central Database and Digital Governance

The digital ID systems that have recently been built in Africa all follow a similar design and vision: to act as a primary form of legal identity that uniquely identifies individuals with a centralised storage of data and governance of the system and to function as a platform for public and private services.[237] The influence of the World Bank here is undeniable:

Through both its internal and external activities, the Bank exerts significant influence in defining what it means to uniquely identify and authenticate a person using digital technology, which technologies and processes are accepted as best practices, and the operational strategies to implement such systems.[238] Meanwhile, at the organisational level, digital ID–related initiatives are now present across multiple practice groups at the Bank, affecting diverse policy and funding areas, including, inter alia, social protection, elections, financial inclusion, and infrastructure. In the case of Nigeria, these were also reinforced by the Agreements, which required FGN to follow ID4D principles and standards in designing NIMC.

Unsurprisingly, the model it defined in these agreements closely resembles that of Aadhaar. The Bank supports, through its line of credit, a foundational ID system that is closely linked to a digitised CR system through the NIN, a unique number.[239]

By digitising the CR and seeding it with the NINs that are issued, as well as by ensuring birth registration also results in NIN generation, the Agreements hope to create a "cradle to grave" ID system.[240] Interestingly, the Financing Agreement defines "ID" to be "an identification that uniquely describes a subject within a given context". It is important to note that several other digital ID systems in the world do not issue unique IDs, allowing a citizen to have more than one mode of identity within the ID system so long as each of them reliably identifies the ID holder.[241] The Aadhaar model, however, is characterised by unique IDs for each resident, since it was intended to address an identified gap – the existence of "fraud" in the development sector – and easier public service delivery.

To achieve uniqueness, both in the ID and in other databases that recorded beneficiaries for government welfare schemes, the Aadhaar system used biometric data to deduplicate entries and tackle identity fraud. This was oft repeated – by the Bank, particularly – as one of the biggest successes of the Aadhaar project, succeeding in weeding out many fraudulent identities.[242] In a study it published, that has since been relied on by the government before the Supreme Court, the Bank discusses how India's digital ID programme can potentially save "over US$11 billion per year in government expenditures through reduced leakage and efficiency gains."[243] However, this claim has been challenged several times by the Indian public,[244] and the over-reliance by Indian policymakers and courts on this statistic has been heavily criticised.

Similarly, in the Agreements, the Bank seeks to enhance NIMC's deduplication capacity and requires that it be integrated into other public sector databases to achieve similar goals. It claims,

> "Nigeria's 2018 budget shows the equivalent of US$5.8 billion in expenditures committed to personnel costs and US$970 million for pensions; even if the introduction of the foundational digital ID leads to only a 5 percent reduction in expenditures due to reduced leakages and reduced number of ghost and ineligible beneficiaries, it would mean US$340 million in public savings per year. Thus, integrating the unique, foundational ID with the registries of other programs and agencies delivering G2P payments could potentially generate billions of dollars of savings over the course of the next decade, from reduced fraud and improved targeting of beneficiaries.[245]

c. Using Digital ID as a Tool to Enable Access to Services

Although the main goal of establishing the NIMC system was to deliver reliable identity services to citizens who otherwise do not have access to IDs, especially in countries with weak or underdeveloped CRV systems, the Bank reinforced (in the Agreements) the need to ensure that the ID also serves as a platform to deliver key services. This was done ostensibly to make such services more accessible to the disadvantaged and to incentivise the uptake of the ID by citizens.[246]

The Bank's vision in the Agreements is to have public and private services be built on the foundation of reliable identity authentication, much like Aadhaar and IndiaStack, UPI, eKYC, etc. To incentivise the uptake of NINs and amplify their developmental impact, the Agreements require the identification of key services that can benefit most from the foundational ID and reliable identity authentication of individuals at the point of service or transaction.
Potential service sectors under this component include financial inclusion (strengthening "know-your-customer" [KYC] for bank accounts and access to credit and insurance), health and social protection programmes (which require ID to verify beneficiaries), education (where a birth certificate is often an admission requirement), and mobile communications (for SIM card registration).[247] The Bank's emphasis on the development of authentication services with the NIN has the goal of creating a federation of public and private entities who can use these services or issue-derived authentication services based on them. It hopes to, with continued investments, "entrench the foundational ID system as indispensable for developing a vibrant, inclusive, and safe digital economy in Nigeria."[248]

Also relevant is the Bank's intention to mainstream the use of the NIN through its other operational engagements with the FGN in the financial and social sectors:

> "This includes the World Bank Group initiatives with the financial sector on regulation and financial inclusion to ensure that NIMC's services are relevant for the financial sector moving forward and integration with the bank verification number (BVN) is accomplished. In the social protection sector, the World Bank currently supports the National Social Safety Nets Project (NASSP) (P151488) which delivers targeted cash transfers to poor and vulnerable households across Nigeria through an electronic payments system using mobile wallets and payment agents. NASSP is building a National Social Registry of poor and vulnerable households to include the NINs of every individual in the registry. The payment services providers engaged under NASSP are natural enrolment partners in the ecosystem approach. The National Social Investments Office has also expressed interest in supporting enrollment in the NIN for other programs such as the school feeding program. Additionally, the World Bank-supported Basic Health Care Provision Fund has also expressed interest in becoming one of the first enrollment partners in the ecosystem.[249]

It is also important to remember here that this system is still, at its core, meant to function as a basic source of legal identity for Nigerians worldwide. In the strategic roadmap created by FGN with the World Bank, it is recommended that the ID system be closely linked with security agencies, including defence, immigration, police, and prisons as a means to identify persons as well as private sector organisations including banks, telecommunications service providers, and health centres that similarly require authentication services.[250]

It also recommended that the system be used for international travel, to promote cross-border free movement of people, regional trade and commerce, & as a regional digital economy.[251] This promotes the collection of large amounts of data that is now accessible to a wide range of actors. Even if sufficient safeguards were put in place to protect this data, controlling its access and preventing security breaches will prove to be a gargantuan task for the FGN.

d. Biometrics as the Only Identifier

The Nigerian ID system envisioned the use of a multi-application smart card as an identifier for citizens to use their digital ID.[252] However, the Agreements stressed on simply considering a biometric identifier, as it would be a way to cut the initial costs associated with building an ID system.

> "The most significant costs associated with ID systems arise from the issuance of sophisticated authenticators (for example, a smart card) and the large number of full-time staff hired, particularly for the initial (mass) enrollment of the population. Thus, digital ID systems could, under certain conditions, benefit from … providing a basic, no-frills authenticator can be sufficient to verify beneficiaries' identity to access many services, while services and transactions requiring a higher level of identity assurance can make use of remote, biometric authentication against the foundational registry.[253]

This was also inspired by the low initial costs that the Aadhaar project had incurred in setting up its system and enrolling users, and the fact that it has been referenced frequently as an instructive case to be followed in the African context.[254]

Although biometrics were always under consideration in the vision for this ID system, the use of biometric data for authentication purposes instead of a smartcard does open the door to increased collection of biometric data at every use by the ID holder during transactions. It also increases the number of actors who collect biometric data from ID holders.

e. Ecosystem Approach and Use of Private Parties in the System

Based on the low initial costs involved in building the Aadhaar system, this contract insists on the adoption of the "ecosystem approach" for enrolling citizens and issuing NINs. It requires that registration be conducted by various (private and public) agencies using an ecosystem approach, integrating a pay-per-enrolment design, which both offsets the costs of enrolment and incentivises the performance of ecosystem partners.[255]

It cites India's experience with this approach, which allowed it to enrol over a billion residents in under five years, and suggests that it would be successful in addressing the large population in Nigeria as well.[256] Because payments are only made based on successful enrolments that culminate in successful deduplication and NIN issuance, ecosystem partners are only paid when new persons are brought into the ID system.

However, this seemingly failed to acknowledge the widespread problems of fraud, transparency, and accountability that were part of the Indian experience with the ecosystem approach. In India, thousands of people were cheated by corrupt private enrollers, with over 50,000 fraudulent operators being subsequently blacklisted.[257]

Limited supervision and transparency also introduced problems of trust in the reliability of Aadhaar identification.[258] It is also worth noting that the Nigerian ID system was once impacted by allegations of corruption over the contracting of a private service provider and had to be immediately suspended.[259]

f. Linking the Digital ID to Key Services to Entrench it into Nigerian Life

The Aadhaar has become almost indispensable to residing and transacting in India, despite the repeated emphasis on its "voluntary" nature.[260]

This was largely the result of two simultaneous practices: first, the Aadhar ID was initially made mandatory to open a bank account, register a SIM card, access education scholarships, receive government subsidies or welfare, pay taxes, etc,[261] (currently, the latter two are still mandatory with limited exceptions); second, Aadhaar has become the default proof of identity; despite laws that say otherwise, most transacting parties require proof of Aadhaar, making life extremely inconvenient for Aadhaar-less residents.[262]

Notwithstanding this experience in India, it seems to be the goal of the actors investing in the Nigerian digital ID system to do exactly this – have the digital ID be indispensable to life in Nigeria. The Agreements recommended a nearly identical approach to incentivise the uptick of NINs, focusing on the same services:

> “Using it for know your customer [KYC] for bank accounts and access to credit and insurance, health and social protection programs that require ID to verify beneficiaries, education, where a birth certificate is typically an admission requirement, and mobile communications, for SIM card registration.[263]

The goal, as repeated often in the Agreements, is to increase the number of people with NINs and to “entrench the foundational ID system as indispensable for developing a vibrant, inclusive, and safe digital economy in Nigeria”.[264] This is also widely evident in the Strategic Roadmap, where the FGN is recommended to prioritise certain important use cases, such as “safety net, financial inclusion, and elections” to help drive the adoption and success of the programme.[265]Although it is not being recommended that authentication through NIN is mandatory for these services, focusing on the key functions that essentially govern a resident’s daily life – particularly those of vulnerable/disadvantaged citizens – has the goal of replicating an Aadhaar-like situation, where life becomes inconvenient for a resident not part of the NIN system.

In India, entrenching the Aadhaar ID with such essential services has caused mass exclusion for Indians with devastating effects, despite India’s Supreme Court mandating that alternatives be allowed for those who do not have an Aadhaar ID.[266] This has, unfortunately, also been the experience of other developing states that have linked similar services to their digital identity systems.[267]

g. Safeguards Instituted and their Impact

The Agreements, along with other publications and reports of these developmental actors, have continuously highlighted the need for a “good” digital ID that mitigates the harms of surveillance, privacy, and exclusion, with appropriate safeguards. To that extent, the existence of a data protection law and other governing regulations were set as conditions for the disbursement of funds.[268]

The Financing Agreement does not allow the withdrawal of funds unless an appropriate data protection bill is enacted,[269] and amendments are made to the NIMC Act,[270] which include limiting NIMC’s authority to share personal data, increasing the range of people who can receive NINs, reducing barriers to registration, removing the compulsion of authentication by NIN, allowing individuals to use alternate means to identify themselves, etc.[271] Specifically, until most of the population has been registered, it recommends that the FGN not restrict access to services for the lack of having NIN as that can exclude especially vulnerable residents, and instead recommends a more organic approach to incentivising the uptake of NINs in Nigeria.[272] Once there is a critical mass of ID holders, it envisions a natural demand from service providers to use the IDs to authenticate their customers and beneficiaries.

By introducing a "unique" ID system essentially meant to replace all the other co-existing functional systems, this design encourages surveillance and exclusion even in the existence of such safeguards.

For example, in India, where both the law and the apex court in the country categorically allow for alternate IDs to be used for access to key services, there have still been widespread and devastating exclusionary impacts. Aadhaar has become a default ID with now growing applications (recently including its linkage with voter IDs)[273] that have raised several causes of concern.

Similarly, it is difficult to anticipate the future of the Nigerian ID system, as the influence of the World Bank is limited by a time period congruent with its financing. There has already been distrust in the FGN's intentions behind some choices concerning the ID system by the Nigerian public,[274] and its current mandatory requirement to access several key services is a cause of concern for the consequences of the Bank's influence weaning.[275] While these safeguards may be useful in the short run, the impact felt by creating this ID system and entrenching it so closely with daily life may be felt by Nigerian residents for many years to come.

Analysis

Norm or policy diffusion is generally understood as a process through which norms, both domestic and international, are taken from one political context and applied to the development of policies, institutions, or ideas in a different political context. The literature on diffusion implies that the spreading, dispersion, and dissemination of ideas or practices from a point of origin happens organically or "contagiously". However, the role of agency and choice in this transfer process, along with the circumstances and environment that influenced the decision-makers, paint a different picture: these transfers may be voluntary or coercive or combinations thereof.[276]

Policy transfer, although similar in effect, refers to political actions that use "knowledge about policies, administrative arrangements, institutions and ideas in one political system (past or present)" in the development of policies, administrative arrangements, institutions, and ideas in another political system.[277]

In our study, we found that there was a transfer and(/or) diffusion of ideas that culminated in influencing domestic policies in developing countries in Africa towards a digital government agenda. This report also looked at the key actors involved in the mechanics of policy transfer, which typically included international and intergovernmental organisations and non-state actors such as interest groups, think tanks, consulting firms, private vendors, and banks. These actors have been shown to have considerable agenda-setting influence when they function as part of "transnational advocacy networks."

Through our research, we found the following influential impacts of international actors on realising the digital ID and digital government agenda, and in guiding domestic ID policies, in developing countries:

1. Through Hard Power Tools of Policy Transfer:

A powerful source of authority for international/intergovernmental organisations is conditionality. Conditionality requires states to alter domestic policy in exchange for funding.[278]

We identified this as the means through which the World Bank encouraged biometric identification and centralisation of data in several countries – most notably, Kenya and Nigeria. In Kenya, the Bank funded the government's main welfare policies on the condition that they are centralised into a single platform, with beneficiary data stored in a single registry, and welfare is only accessible through a unique biometric identification system.[279] This was intended to improve targeting benefits/subsidies to eligible beneficiaries only and minimise leaks in the welfare system. Through subsequent conditional loans, the Bank ensured the integration of this social registry into other key nationwide identification systems, simultaneously increasing its scope and coverage. Eventually, this led to the current NIIMS system that integrates population registration with welfare management, which was quickly endorsed by the World Bank.

In Nigeria, this impact was significantly more transparent: The agreement that governed the funding of Nigeria's ID system offered to the FGN has several conditions – spanning the design, technicalities, and regulations of the digital ID system.[280] As a result of this, Nigeria's current digital identification policy, including its regulatory environment, is largely influenced by the World Bank.

2. Soft Power Tools of Policy Diffusion:

In contrast, soft power tools exert influence through the establishment of norms that nudge actors toward compliance, along with the proffering of policy models or "best practices".[281] In some cases, the influence of actors is authoritative because of their perceived legitimacy on policy matters and expertise (such as in the case of the OECD).[282] This may result in policymakers relying on the expertise of these actors to create and assess policies and monitor their compliance with agreed-upon conventions and rules.

In our research, we identified several different ways in which soft power tools influenced the "Aadhaar digital ID agenda" in the countries we looked at:

a. **The World Bank's technical and policy assistance:** In both Nigeria and Kenya, the Bank wrote extensive diagnostic reports about the identification systems that existed in the countries and how they could be improved to tackle existing administrative problems. In the case of Nigeria, the Bank worked closely with the FGN to create a "strategic roadmap" for the future of digital identification in Nigeria and even offered technical assistance during the implementation of the NIMC system.[283]

b. **Research produced:** The World Bank plays a significant role in framing policy discussions and setting agendas around national digital ID systems, through its ID4D initiative. To this end, the initiative has published research on digital ID systems, covering everything from basic terminology, technology systems and technical standards, cost models, principles for sustainable development, linking digital ID and development/inclusion goals, etc.[284] Through these, the Bank exerts significant influence on what digital IDs comprise, best practices for identifying and authenticating citizens, and digital governance mechanisms. In the scope of our study, the Bank's "Digital Identity Toolkit for Africa" and "Principles on Identification for Sustainable Development" are significant examples of the Bank's influence through the prescriptive models they offer for developing countries in Africa to use digital governance to address their unique problems. In light of the different ideas and concepts of digital ID and digital governance, this research not only solidifies a digital ID agenda, but also popularises a specific model of digital ID for "development".

c. **Advocacy networks, conferences, workshops:** ID4D and its subchapters such as ID4Africa along with private sector finance/technology companies, state bodies, intergovernmental organisations, and philanthropic organisations function as an advocacy network that has a significant influence on the decision-making involved in implementing national digital ID systems. As seen on page xyz, conferences and alliances organised through the network have the impact of setting certain trends and encouraging specific activities; as these are also typically directed at policymakers, their influence is not negligible. The constant presence of officials from the Aadhaar/UIDAI programme further evinces the network's intention to replicate an Aadhaar-adjacent digital ID model with similar goals and effects.

d. **Uncritical presentation of Aadhaar:** Aadhaar's apparent success in addressing the developmental problems in India is frequently presented as a solution to other developing states, particularly in Africa, with inadequate focus on the harms that the system has brought. With Aadhaar having been operational for many years now, much evidence about its devastating impact and the exclusionary, privacy, security, and surveillance risks it introduces has been unearthed, but little of this knowledge accompanies presentations on Aadhaar in global forums. The influence of this distorted representation of the Aadhaar model on state policymakers has been significant in advancing the digital ID agenda globally.

Conclusion

The reliance on digital identity to solve larger problems of poverty, corruption, exclusion, and political instability is another case of tech solutionism that could potentially be accompanied by severe risks. What we hope is taken from this research is the impact of external influences on key policy decisions regarding the nature and reach of national biometric civil registration/identification systems. Many incentives co-exist in the creation of national digital ID systems; often, while the developmental purpose of such a system is widely known, the numerous other profit motives and influences are rarely discernible to the ordinary citizen.

These actors involved in pushing the digital ID agenda urge national governments to become providers of identification services and holders of vast amounts of personal information, typically at the expense of immense costs borne by taxpayers. The economic benefits of these programmes, though easily claimed, are not well-documented and are often disputed.

In the future, we hope to augment this research with a deeper focus on the incentives and business models of supranational development organisations, global consultancy firms, and technology-vendor alliances. We also hope to focus on specific case studies and work with local researchers to explore the influence that international actors have had on their domestic policy in more detail and with the appropriate cultural and political contexts.

Endnotes

1 Colin Bennett and David Lyon, Playing the Identity Card: Surveillance, Security and Identification in Global Perspective (Routledge, 2008).
2 Aaron Martin, "Aadhaar in a Box? Legitimizing Digital Identity in Times of Crisis", Surveillance & Society19, no. 1 (2021): 104–108. research.tilburguniversity.edu
3 "Report to the Congress: U.S. Immigration Policy: Restoring Credibility Executive Summary", U.S. Commission on Immigration Reform, 1994; "The President's Health Security Plan: The Clinton Blueprint", The White House Domestic Policy Council Staff (Times Books, 1993); Steve Young, "Americans Mull National ID Cards," CNN, October 31 2001.
4 Pew Research Center, " American Psyche Reeling from Terror Attacks", 19 September 2001, pewresearch.org
5 "Biometrics Collection under the Pretext of Counter-terrorism", Privacy International, accessed 17 March 2022, privacyinternational.org.
6 Alan Gelb and Julia Clark, "Identification for Development: The Biometrics Revolution", Working Paper 315, Center for Global Development (2013): www.cgdev.org; Silvia Masiero & Savita Bailur, "Digital Identity for Development: The Quest for Justice and a Research Agenda", Information Technology for Development 27 (2020): 1– 12, doi.org.
7 Aaron Martin and Linnet Taylor, "Exclusion and Inclusion in Identification: Regulation, Displacement and Data Justice." Information Technology for Development 27, no.1 (2021): 50–66, doi.org
8 16.9, Sustainable Development Goals, Transforming our World: the 2030 Agenda for Sustainable Development, 2015.
9 "Home", Identification for Development, The World Bank Group, accessed 17 March 2022, id4d.worldbank.org
10 "Home", India Stack, accessed 17 March 2022, indiastack.org
11 K. S. Puttaswamy v Union of India (2019) 1 SCC 1, paras 314, 373.
12 "Annual Report 2017–18," Unique Identification Authority of India, 2018, uidai.gov
13 Nikhil Pahwa, "Lessons from Aadhar: 10 Rules for Nations on How Not to Make a Mess of their National IDs", The Scroll, 27 Nov 2017, scroll.in
14 Anand Venkatanarayan, "The Curious Case of the World Bank and Aadhaar Savings", The Wire, 03 October 2017,wire.in; Reetika Khera, "On Aadhaar Success, It's All Hype – That Includes the World Bank", NDTV, 25 July 2016, www.ndtv.com.
15 Reetika Khera, Dissent on Aadhaar: Big Data Meets Big Brother (Orient BlackSwan, 2018); Haki na Sheria Initiative (Garissa), "Biometric Purgatory: How the Double Registration of Vulnerable Kenyan Citizens in the UNHCR Database Left Them at Risk of Statelessness", Citizenship Rights Initiative Africa, 17 November 2021, citizenshiprightsafrica.org; "Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID", Initiative for Social and Economic Rights, and Unwanted Witness, Center for Human Rights and Global Justice, 8 June 2021, chrgj.org
16 Judicial Trends: How Courts Look at Digital ID Programs", Digital Identities Design and Uses, Center for Internet Society, 20 July 2020. digitalid.design
17 "Notification No. A-43011/02/2009-Admn-I", Government of India Planning Commission, 28 January 2009, uidai.gov
18 The Aadhar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. Demographic data is defined under Section 2(k) of the Aadhaar Act as including information relating to name, date of birth, address, and the option of providing an email address and mobile number. Biometric data is defined under Section 2(g) of the Act and includes photograph, iris scan, and fingerprints.
19 For a detailed understanding of the role of the UIDAI and its regulatory and quasi-judicial

functions, see Vrinda Bhandari and Renuka Sane, "A Critique of the Aadhaar Legal Framework", 31 NSLIR Rev (2019), 1-23 papers.ssrn.com.
20 Section 2(k) and 3, Aadhaar Act read with Regulation 5 of the Aadhaar (Enrolment and Update) Regulations, 2016.
21 Section 2(g) and 3, Aadhar Act read with Regulations 3 and 6 of the Aadhaar (Enrolment and Update) Regulations, 2016.
22 Regulation 5, Aadhaar (Enrolment and Update) Regulations, 2016.
23 K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1, 1351. The Court recorded the submissions of Mr. Rakesh Dwivedi, Sr. Advocate, appearing on behalf of one of the Respondents, State of Gujarat.
24 Ibid, at 184
25 "Enrolment Partners/Ecosystem Partners", UIDAI, uidai.gov
26 Id.
27 K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1, para 184.
28 Id., 247.
29 Id., 247.
30 Id., 247
31 Id., 247.
32 "Requesting Entities", UIDAI, uidai.gov
33 "Authentication Service AUA KUA", Karnataka Resident Data Hub, ceg.karnataka.gov.
34 K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1, 1336.
35 Id.
36 Id., 184.2.
37 "List of Live Authentication Service Agencies (ASAs)", UIDAI, August 2018, uidai.gov
38 Harsimran Julka, "HCL Infosystems wins Aadhaar contract of Rs 2,200 crore from UIDAI", Economic Times, 02 March 2012, economictimes.indiatimes.com. See also, "Wipro given undue favours in Aadhaar project, says CAG report, Hindu Businessline, 17 January 2018, thehindubusinessline.com
39 "Sebi lists 8 entities that can undertake e-KYC Aadhaar authentication", Business Standard, 12 May 2020, business-standard.com.
40 K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1, 1348.
41 Government of India, Ministry of Electronics and Information Technology, "Availability of Aadhaar Data with Private Companies", 25 July 2019, uidai.gov
42 FIR No. 278/19, PS Cyberabad, available at medianama.com.
43 Jeanette Rodrigues, "India ID Program Wins World Bank Praise Despite 'Big Brother' Fears", Bloomberg, 16 March 2017, bloomberg.com; also read "Afghan Officials Get Exposure to Aadhaar Process", The Indian Express, 3 January 2020, newindianexpress.com
44 "Covid-19 Spurs National Plans to Give Citizens Digital Identities", The Economist, 7 December 2020, economist.com
45 Rodrigues, supra note 43. See also "Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable", The World Bank, 14 August 2019, worldbank.org.
46 World Bank, "World Development Report, 2016: Digital Dividends", Washington DC, 2016, worldbank.org, at 27–28, 194.
47 Mariana Dahan and Alan Gelb, "The Role of Identification in the post-2015 Development Agenda", Working Paper, The World Bank, 2015, openknowledge.worldbank.org, at 6. See also World Bank, "Digital Dividends", supra note 23: 195.
48 World Bank, "Digital Dividends", supra note 46: 2.
49 "Quote – Unquote", Unique Identification Authority of India, uidai.gov; Rodrigues, supra note 43.
50 "Guidance Note on ID Enabling Environment Assessment (IDEEA)", Identification for Development, The World Bank, 15 May 2019: 49, documents1.worldbank.org
51 Id.: 17, 21, 63, 76.
52 Shiv Sahay Singh, "Death by Digital Exclusion? On Faulty Public Distribution System in Jharkhand", The Hindu, 13 July 2019, thehindu.com; Aria Thaker, "Aadhaar Security Failure:

Government Webpages Provide Unsecured Access to Demographic Authentication", The Caravan, 22 June 2018,caravanmagazine.in; Ashwini Deshpande, "Aadhaar and My Brush with Digital Exclusion", The Wire, 3 January 2022, thewire.in.

53 Section 7 of the Aadhaar Act, 2016.

54 Siraj Dutta, "Exclusion by Biometric", The Indian Express, 18 July 2021, indianexpress.com

55 Jean Dreze et al., "Balancing Corruption and Exclusion: A Rejoinder", Ideas for India, 28 September 2020, ideasforindia.in.

56 Dalberg, "State of Aadhaar: A People's Perspective", 2019 edition, stateofaadhaar.in (funded by Omidyar Network).

57 Yogesh Sapkale, "Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast", MoneyLife, 19 February 2019, moneylife.in; "Aadhaar Security Breaches: Here are the Major Untoward Incidents that have Happened with Aadhaar and what was Actually Affected", FirstPost, 25 September 2018, firstpost.com

58 World Bank, "Digital Dividends", supra note 46: 194.

59 Sreedevi Jayarajan, "No Such Rule, but Many Vaccination Centres are Insisting on Aadhaar as Proof", The News Minute, 4 June 2021, thenewsminute.com; While registering for vaccinations at the online portal, one is required to produce the same government id as a proof of authentication. This was not observed by many hospitals that demanded Aadhar as valid identity proof. The Supreme Court in a recent order has said that producing Aadhar cards was not mandatory for vaccination. Also note, "11 Documents to be Used as Identity Proof for Voting", The Hindu, 18 February 2022, thehindu.com; and Aria Thaker," Aadhaar's Most Common Use Is also One of its Most Dangerous Problems", Quartz India, 25 September 2018, qz.com.

60 "Identity in a Digital World: A New Chapter in the Social Contract", World Economic Forum, September 2018: 13, 16, 21,, www3.weforum.org, at 13, 16, 21

61 For example, the World Economic Forum's Report titled "Digital Identity Ecosystems: Unlocking New Value" notes that 88% of India's population uses Aadhaar. See "Digital Identity Ecosystems: Unlocking a New Value: An Interactive Guide for Executives", 2021: 49, www3.weforum.org.

62 WEF (2018), supra note 61: 21.

63 "Nandan Nilekani at Davos: Faced Lot of Unknowns when Aadhaar Work Began, Issues R esolved Now", The India Today, 25 January 2019,indiatoday.in

64 WEF (2021), supra note 61: 21.

65 Id.: 10, 56.

66 "Home", ID4Africa, accessed 17 March 2022, id4africa.com

67 "Presentation at the 5th Annual Meeting of the ID4Africa Movement", News & Events, MOSIP, accessed 17 March 2022, mosip.io; "MOSIP Features in ID4AFRICA's Livecast on Digital Public Goods Initiatives as Pathways to Identity Development", News & Events, MOSIP, accessed 17 March 2022, mosip.io.

68 Rajesh Bansal, Id.:32, id4africa.com. For event schedule and designation, see here

69 Id.

70 Id. DigiLocker is an initiative by the government that aims at providing access to "authentic digital documents to the citizen's digital document wallet." See DigiLocker, digilocker.gov

71 Mardav Jain, "The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment", The Henry M Jackson School of International Studies, University of Washington, 9 May 2019, jsis.washington.edu ; Also read Reetika Khera, "The Different Ways in which Aadhaar Infringes on Privacy", The Wire, 19 July 2017,thewire.in; Vrinda Bhandari and Renuka Sane, "A Critique of the Aadhaar Legal Framework", 31 NSLIR Rev (2019): 1– 23, papers.ssrn.com; Vrinda Bhandari, Shruti Trikanad, and Amber Sinha, " Governing ID: Principles of Evaluation", Centre for Internet & Society, Digital Identities Project 2020, available at SSRN: ssrn.com.

72 Rahul Lahoti, "Questioning the 'Phenomenal Success' of Aadhaar-linked Direct Benefit Transfers for LPG", The Economic and Political Weekly 51, Issue No. 52 (2016) epw.in

73 Anit Mukherjee, "ID and Service Delivery: Emerging Evidence and Lessons from India", Center for Global Development (2019), id4africa.com. For events programme, see "Theme:

Identity Ecosystems for Service Delivery", The 5th Annual Meeting of ID4Africa Movement, 18 June 2019, id4africa.com.
74 Id : 33. While the presentation noted that it was the Center for Global Development's estimate that digital reforms had led to fiscal savings, it acknowledged that savings from Aadhaar were a "contentious" issue.
75 Id.
76 Aayushi Rathi and Ambika Tandon, " The Digital Identification Parade", The Center for Internet and Society, 30 July 2019, cis-india.org ; Also read Karen Hao, "This is How we Lost Control of Our Faces", MIT Technology Review, 5 February 2021, technologyreview.com; and Shubhajit Basu and Rhyea Malik, "India's Dodgy Mass Surveillance Project Should Concern U s A ll", The Wired, 25 August 2017, wired.co.uk.
77 Saïd Aït-Hatrit, "Biometric Identification: A Coveted African Market ", Acuity Market Intelligence, 22 June 2018, theafricareport.com.
78 "There are only four or five of us competing on the global market, even if other companies may be able to compete locally for technical or political reasons," explains Ronny Depoortere, vice-president of Zetes' People ID division, Id.
79 "About Us ", Thales, accessed 20 March 2022, web.archive.org://www.thalesgroup.com.
80 "Digital Identity and Security ", Thales, accessed 20 March 2022, thalesgroup.com.
81 "Nigerian N ational ID P rogram: A n A mbitious I nitiative ", Thales, accessed 19 March 2022, thalesgroup.com.
82 "Thales Completes Acquisition of Gemalto to Become a Global Leader in Digital Identity and Security", Thales, accessed 20 March 2022, thalesgroup.com
83 Id.
84 Aït-Hatrit, 2018 supra note 77.
85 Id.
86 "Next Generation Digital Security: Annual Report 2018", Gemalto, thalesgroup.com
87 "Nigeria Retains Safran Identity & Security to Provide an Upgraded Automatic Biometric Identification System and Maintenance", IDEMIA, last accessed 19 March 2021, idemia.com
88 Musembi Mutisya, "The Huduma Number – Digital Identity and Inclusion in Kenya", Pesacheck, 7 June 2019, pesacheck.org
89 Justin Lee, "OT-Morpho Denies Claims Kenyan Biometric Voting System was Hacked", Biometric Update, 19 September 2017, biometricupdate.com
90 Keren Weitzberg, "Kenya's Controversial Biometric Project Is Shrouded in Secrecy", Codastory, 3 May 2019, codastory.com
91 Luana Pascu, "IN Groupe Nexus Acquisition and Ubisecure Partnership Expand Digital ID Services in Europe", Biometric Update, 6 February 2020, biometricupdate.com
92 Justin Lee, "Imprimerie Nationale Group Delivers Multi-Biometric ID Documents Platform for Republic of Djibouti,", Biometric Update, 10 February 2017, biometricupdate.com
93 Chris Burt, "Monaco Choses IN Groupe to Secure Digital Identity, Produce Biometric Identity Documents", Biometric Update, 16 October 2020, biometricupdate.com
94 Chris Burt, "Mühlbauer Helps Uganda Reach 30M Biometric Registrations, Details Mozambique and Fiji Projects", Biometric Update, 10 October 2020, biometricupdate.com
95 Aït-Hatrit, 2018 supra note 77.
96 Aït-Hatrit, 2018 supra note 77 for more.
97 "Our Mission", Security Identity Alliance, last accessed 19 March 2022, secureidentityalliance.org
98 Id.
99 Luana Pascu, "Idemia and IN-Groupe Executives to Lead Secure Identity Alliance Board," Biometric Update, 17 January 2020, biometricupdate.com
100 "Past Events", Security Identity Alliance, last accessed 19 March 2022 secureidentityalliance.org
101 See "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation", World Bank Group – GSMA – Secure Identity Alliance Discussion Paper, 1 July 2016, documents.worldbank.org

102 "The OSIA initiative", OSIA, last accessed 19 March 2022, secureidentityalliance.org
103 "Putting Government Back in Control: Solving Vendor Lock-in with Open Standards", Security Identity Alliance, 2019, id4africa.com
104 Id.; See also "Open APIs as a Pathway to Identity and Sectoral System Development", ID4Africa Livecast, 28 January 2022, id4africa.com
105 "About MOSIP", MOSIP, accessed 17 March 2022, mosip.io
106 Id.
107 "MOSIP: Home", MOSIP, accessed 17 March 2022, mosip.io
108 Id.
109 Id.
110 The Economist, supra note 44.
111 Id.
112 Id. See also Shradha Sharma, "[YS Exclusive] Nandan Nilekani on Why Scale Matters, His 'Big Dream,' and More", YourStory, 19 September 2019, yourstory.com.
113 "Bill Gates Cites MOSIP as Pathway and Enabler of Digital Financial Inclusion in Interview with CNBCTV18", News & Events, MOSIP, 15 December 2020.mosip.io; "India Has Shown Digital Financial Inclusion Is Possible: Bill Gates", CNBC TV18, accessed 17 March 2022, cnbctv18.com.
114 The Economist, supra note 44.
115 "The Government of The Togolese Republic Sign an MoU with IIIT-B on MOSIP", News & Events, MOSIP, accessed 17 March 2022, mosip.io
116 "The Philippine Statistics Authority (PSA) Crosses Critical Milestones for the Philippine Identification System (PhilSys)", News & Events, MOSIP, accessed 17 March 2022, mosip.io; "MoU between Government of Morocco and IIIT-B", News & Events, MOSIP, accessed 17 March 2022, mosip.io
117 Id.: 61; also read "MOSIP Enters Partnership with Sri Lanka on D igital ID S ystem", News & Events, MOSIP, accessed 17 March 2022, mosip.io
118 "IIIT-B & Ministry of Peace, Federal Democratic Republic of Ethiopia S ign MoU on MOSIP", News & Events, MOSIP, accessed 17 March 2022, mosip.io
119 MOSIP, supra note 67.
120 "MOSIP Features in ID4AFRICA's Livecast on Digital Public Goods Initiatives as Pathways to Identity Development. Watch the R ecording", News & Events, MOSIP, accessed 17 March 2022, mosip.io.
121 "MOSIP Presents During UN General Assembly 2019", News & Events, MOSIP, accessed 17 March 2022, mosip.io.
122 "People", MOSIP, last accessed 17 March 2022, mosip.io.
123 Id.
124 "Our Missions and Values", CIVIPOL, last accessed 19 March 2022, civipol.fr.
125 "Missions and Projects", CIVIPOL, last accessed 19 March 2022, civipol.fr
126 "Identity, Missions and Projects", CIVIPOL, last accessed 19 March 2022, civipol.fr
127 "Our Missions and Values", CIVIPOL, last accessed 19 March 2022, civipol.fr.
128 "Senegal: Support Programme to Strengthen the Civil Registration Information System and Consolidation of National Biometric Identification Database", CIVIPOL, last accessed 19 March 2022, civipol.fr
129 "EU Emergency Trust Fund for Africa", European Commission, last accessed 19 March 2022,ec.europa.eu.
130 "Support Programme for the Running of the Civil Registration System in Mali: Support for the Implementation of a Secure Information System",
CIVIPOL, last accessed 19 March 2022, civipol.fr.
131 "Support for the Implementation of Côte D'Ivoire's National Civil Status and Identification Strategy", CIVIPOL, last accessed 19 March 2022, civipol.fr.
132 "The European Union Supports the Modernization of Civil Status in CAR", CIVIPOL, last accessed 19 March 2022, civipol.fr.
133 "Missions and Projects", CIVIPOL, last accessed 19 March 2022, civipol.fr.
134 "Here's how a Well-connected Security Company is Quietly Building Mass Biometric

Databases in West Africa with EU Aid Funds", Privacy International, 10 November 2020, privacyinternational.org
135 Id.
136 Id.; Olivia Baker, "Biometric Tech Used to Return African Migrants from EU, Privacy International Reveals", Identity Review, 19 November 2020, identityreview.com
137 "Challenging the Drivers of Surveillance: EU Access to Documents Requests EUTF for Africa Disclosures", Privacy International, November 2019, privacyinternational.org
138 Id., Doc 3.3: 4.
139 Madeleine Speed, "Activists Sound Alarm over African Biometric ID Projects", Aljazeera, 10 December 2020, aljazeera.com
140 Grace Mutung'u, "Digital Identity in Kenya: Case Study Conducted as Part of a Ten-country Exploration Of Socio-digital ID Systems in Parts of Africa", Research and ICT Africa & Centre for Internet & Society (2021): 10, digitalid.design.
141 "The Digital Transformation Strategy for Africa (2020–2030)", Africa Union (2020): 39–42, au.int
142 "Identity for Development Country Diagnostic: Kenya", The World Bank, 2016, documents1.worldbank.org
143 Id.: 1.
144 "National Safety Net Program for Results", Projects and Operations, The World Bank, accessed 17 March 2022, projects.worldbank.org
145 "Program Appraisal Document on Proposed Credit in the Amount of SDR 166.9 Million to the Republic of Kenya for National Safety Net Program for Results", World Bank, 26 June 2018, documents1.worldbank.org
146 Id.
147 "Implementation Completion Report (ICR) Review", Independent Evaluation Group, National Safety Net Program, World Bank, 31 Dec 2020, documents1.worldbank.org.
148 Id.
149 "Kenya Cash Transfer for Orphans and Vulnerable Children", Projects and Operations, World Bank, accessed 17 March 2022, projects.worldbank.org
150 "Implementation Completion and Results Report on a Credit in the Amount of SDR 33 million and an Additional Credit of in the Amount of SDR 6 million to the Republic of Kenya for a Cash Transfer for Orphans and Vulnerable Children Project", The World Bank, 19 June 2019, documents1.worldbank.org
151 Id.
152 Id.: 17.
153 Id.
154 "Project Appraisal Document on a Proposed Credit in the A mount of Euro 215.9 Million to the Republic of Kenya for the Kenya Social and Economic Inclusion Project", World Bank, 2 November 2018, documents1.worldbank.org.
155 Id., note Component 1, Strengthening Social Protection Delivery Systems.
156 Id. : 11.
157 "World Bank A pproves $750 Million for Kenya in Support o f Reforms i n Agriculture, Housing, Digital Technology a nd Fiscal Management", World Bank, 28 May 2019, worldbank.org
158 Programme Document for a Proposed Development Policy Credit in the Amount of SDR 540.3 million to The Republic of Kenya for the Kenya Inclusive and Fiscal Management Development Policy Financing", The World Bank, 29 April 2019, documents1.worldbank.org.
159 Id.
160 "Financing Agreement (Inclusive Growth and Fiscal Management Development Policy Financing) B etween the Republic of Kenya and International Development Association", The World Bank, 19 June 2019, documents1.worldbank.org.
161 Id.: 7.
162 Programme Document for a Proposed Development Policy Credit 2019 supra note 158: 88.

163 Practitioners Guide, Identity For Development", The World Bank Group, October 2019, documents1.worldbank.org, 79.
164 Id.
165 "About", Huduma Namba, accessed 18 March 2022, hudumanamba.go.ke; See also Nubian Rights Forum and 2 others v AttorneyGeneral and 6 others; Child Welfare Society & 9 Others (Interested Parties), Petition No. 56, 58, and 59 of 2019 (c onsolidated) decided by the Kenyan High Court in January 2020, [2020] eKLR, khrc.or.ke [hereinafter referred to as "NIIMS judgement"], paras 1 and 2.
166 Robert Mugo, "Kenya National Integrated Identity Management Systems", ID4Africa, accessed 18 March 2022, id4africa.com; Agenda is id4africa.com; hudumanamba.go.ke.
167 Section 9A, The Registration of Persons Act, 1947, as amended in 2018.
168 Huduma Namba, supra note 165.
169 Mugo, supra note 166.
170 Id.
171 Nubian v. Kenya & Ors, para 1047.
172 The Huduma Regulations consist of the Registration of Persons (NIIMS) Rules, 2020, and the Data Protection (Civil Registration) Regulations, 2020. See Mutung'u, supra note 140.
173 Republic v. Joe Mucheru [2021] KEHC 122 (KLR).
174 Mutung'u, supra note 140, at 11.
175 "Kenya's National Integrated Identity Management System", Open Society Justice Initiative, March 2020, justiceinitiative.org
176 Id.
177 World Bank (2016), supra note 142: 21.
178 "Digital Economy Blueprint – Powering Kenya's Transformation", Kenya Digital Economy, May 2019, ict.go.ke.
179 Id .: 73.
180 Nubian v. Kenya & Ors, para 28.
181 Id., at paras 29– 31.
182 K. S. Puttaswamy v Union of India, (2019) 1 SCC 1.
183 Mutung'u, supra note 140: 11, 21.
184 Section 7, Aadhaar Act, 2016 and Section 139AA, Income Tax Act, 1961.
185 K. S. Puttaswamy v Union of India (2019), 1 SCC 1.
186 The Registration of Persons (National Integrated Identity Management System) Rules, 2020. Rule 10 of the NIIMS Registration of Persons states, "Any government agency requiring personal particulars of an individual shall, at the first instance, rely on the NIIMS database to authenticate the foundational data of an enrolled resident individual."
187 World Bank (2016), supra note 142: 5– 6.
188 Id.: 21– 22.
189 Regulations 3– 5 and 17, Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) , 2016.
190 Christian Matthew Phillip, "Aadhaar H elps R ailways T race P arents of T rafficked K ids", The Times of India, 8 November 2017,timesofindia.indiatimes.com.
191 Soumya Kalasa, "244 Children Trafficked to Bengaluru Using Fake Aadhaar Cards", News 18, 15 December 2021, news18.com; S Lalitha, "244 Children Trafficked to Bengaluru had F ake Aadhaar Cards", The Indian Express, 14 December 2021, newindianexpress.com
192 Mutung'u, supra note 140: 14.
193 Nubian v Kenya & Ors, para 537.
194 Mutung'u, supra note 140: 13.
195 Section 2(k), Aadhaar Act, 2016.
196 World Bank (2016), supra note 142: 21.
197 The Statute Law (Miscellaneous Amendments) Act, 2018 (Act No. 18 of 2018).
198 World Bank (2016), supra note 142: 6.
199 Id.: 3, 5, 18.
200 Id..: 20.

201 Section 9A(2)(f), Registration of Persons Act, 1947, as amended in 2018.
202 Mutung'u, supra note 140: 21.
203 "Case Study: Deploying Digital Identity Systems", Paradigm Initiative (2021), paradigmhq.org.
204 Grace Mutung'u, " Kenya's Transition to Digital ID Not Without R isks", Research ICT Africa, 30 July 2021,researchictafrica.net.
205 Nubian v. Kenya & Ors, para 33– 35.
206 Hans Verghese Matthews, "Flaws in the UIDAI Process", Economic and Political Weekly, 27 February 2016, cis-india.org. See also Nubian v. Kenya & Ors, para 34.
207 Nubian v. Kenya & Ors, paras 876, 1010– 1012.
208 "World Development Report 2021", The World Bank, 2021, worldbank.org
209 Id.: 28.
210 Id.: 71.
211 "President Uhuru Defends Integrity of Huduma Namba Project", NTV Kenya, YouTube, accessed 18 March 2022, youtube.com
212 Musembi Mutisya, "The Huduma Number — Digital Identity and Inclusion in Kenya", PesaCheck, 7 June 2019,pesacheck.org
213 Faith Nyaunga Nyakundi, "Huduma Namba: Kenya's Transformation into an Informational State", University of Washington, 2020,digital.lib.washington.edu
214 "Identification for Development: Africa Business Plan (FY 18–20)", The World Bank, 2017, documents1.worldbank.org
215 "Financing Agreement (Digital Identification for Development Project) between Federal Republic of Nigeria and International Development Association", The World Bank, 20 February 2021.
216 See section "International Actors Influencing ID System" above, on page 7.
217 Nicholas Ibekwe, "Nigeria's Troubled National ID Card Project in Fresh Controversy", Premium Times, 27 May 2015, premiumtimesng.com.
218 NIMC presentation, titled "Sagem S.A. France – Closure of 2001 Agreement and Handover of the Nigerian National Identity Card Programme: The Issues", National Identity Management Commission, accessed 18 March 2022, nimc.gov.
219 Final Report of The Committee on Harmonisation of National Identity Cards, Committee on Harmonisation of National Identity Cards, March 2006, nimc.gov
220 Id.
221 Id.
222 Id,
223 Id.
224 Chairman's speech at the Presentation of The Report of the Committee on Citizen Data Management and Harmonisation to Mr President, Government of Nigeria, 13 August 2020, citizenshiprightsafrica.org
225 Id. The committee was convened to "develop systems and processes that would address the security concerns raised by the United States of America as well as work towards the early removal of the restrictions".
226 "Country Engagement", Identity for Development, World Bank, accessed 18 March 2022, id4d.worldbank.org
227 "Identity for Development Country Diagnostic: Nigeria", World Bank, 2016, documents1.worldbank.org.
228 "A Strategic Roadmap for Developing Digital Identification in Nigeria", National Identification Commission of Nigeria, 12 September 2018, nimc.gov
229 Id.: 3.
230 Id.: 12.
231 "Nigeria Digital Identification for Development Project", The World Bank, accessed 18 March 2022, projects.worldbank.org
232 International Development Association Project Appraisal Document on a Proposed Credit in the Amount of SDR 84.4 million to the Federal Republic of Nigeria for Digital Identification

Development Project, 30 January 2020, documents1.worldbank.org
233 "Financing Agreement between Federal Republic of Nigeria and International Development Association", 20 February 2021, documents1.worldbank.org
234 "Sectoral and Institutional Context", International Development Association Project Appraisal Document, 2020 supra note 232: 8.
235 Aman Sharma, "World Bank Approaches Unique Identification Authority of India to Share its Experiences with Other Countries", The Economic Times, 9 September 2016, economictimes.indiatimes.com.
236 Id.
237 See "Digital Id in Africa", Centre for Internet & Society, accessed 18 March 2022, digitalid.design
238 "Research", Identity for Development, The World Bank, accessed 18 March 2022, id4d.worldbank.org
239 "Financing Agreement", 2021 supra note 233, "Schedule 1".
240 "International Development Association Project Appraisal Document", 2020 supra note 232.
241 See the Digital ID systems of the United Kingdom, Canada, etc.
242 "Digital Dividends", World Bank Group, 2016: 195, documents1.worldbank.org
243 Id.
244 Anand Venkatanarayan, "The Curious Case of the World Bank and Aadhaar Savings", The Wire, 3 October 2017,thewire.in; Reetika Khera, "On Aadhaar Success, It's All Hype – That Includes the World Bank", NDTV, 25 July 2016,ndtv.com.
245 International Development Association Project Appraisal Document, 2020 supra note 232: 35.
246 Id., "Component 3: Enabling Access to Services through IDs".
247 Nigeria (World Bank), 2016, supra note 227: 22.
248 Id.: 33.
249 Id.
250 Strategic Roadmap, 2018 supra note 228: 12.
251 Id.
252 Harmonisation Committee, 2006 supra note 219.
253 Nigeria (World Bank), 2016, supra note 227: 29.
254 "Identification for Development: Africa Business Plan (FY 18–20)", The World Bank, 2017, documents1.worldbank.org
255 International Development Association Project Appraisal Document, 2020 supra note 232, Component 2: Establishing a Robust and Inclusive Foundational ID System 306.00.
256 Id.
257 "49,000 Fraudulent Operators Blacklisted, says UIDAI", The Times of India, 12 September 2017, timesofindia.indiatimes.com; "Press Statement", Unique Identification Authority of India, 11 September 2018, uidai.gov
258 Anand Venkatnarayan, "Are People Who Sign up for Aadhaar Actually Who They Say They Are? UIDAI May Not Know", The Wire, 23 July 2018,thewire.in
259 Nicholas Ibekwe, "Nigeria's Troubled National ID Card Project in Fresh Controversy", Premium Times, 27 May 2015, premiumtimesng.com
260 Express Web Desk, "Supreme Court rules Aadhaar not Mandatory for Bank Accounts, Mobile Numbers, School Admissions", The Indian Express, September 2018, indianexpress.com
261 "Big Aadhaar Verdict: Here Is What It Changes", The New Indian Express, 26 September 2018, newindianexpress.com
262 Ananya Bhattacharya and Nupur Anand, "Aadhaar Is Voluntary – but Millions of Indians are Already Trapped ", Quartz India, 26 September 2018, qz.com.
263 "International Development Association Project Appraisal Document", 2020 supra note 232, Component 3: Enabling Access to Services through IDs 66.00.
264 Id.
265 "Strategic Roadmap", 2018 supra note 228: 12.

266 Jean Dreze, "Dark Clouds over the PDS", The Hindu, 10 September 2016, thehindu.com; Dalberg, "State of Aadhaar: A People's Perspective ", 2019, stateofaadhaar.in; "In the Absence of Aadhaar, Starvation Deaths Continue in Jharkhand", Sabrang India, 21 November 2018, sabrangindia.in; Rahul Bhatia, "How India's Welfare Revolution Is Starving Citizens", New Yorker, 16 May 2018, newyorker.com
267 See "Exclusion by Design: How National ID Systems Make Social Protection Inaccessible to Vulnerable Populations", Privacy International, 29 March 2021,privacyinternational.org
268 See International Development Association Project Appraisal Document, 2020 supra note 232, Component 1: "Disbursement conditions will be used to encourage the Government to implement specific legal reforms without which the PDO will be negatively affected. Amendments to particular provisions of the NIMC Act deemed to be critical to the PDO achievement are disbursement conditions on the second tranche of enrollment funds. These provisions include those related to promoting inclusion and non-discrimination, protecting ownership of personal data, access to personal data by third parties, and mandatory use of NIN."
269 Financing Agreement, 2021 supra note 233, Section III (B) (1).
270 Id.
271 Financing Agreement, 2021 supra note 233, Annexure to Schedule 2.
272 International Development Association Project Appraisal Document, 2020 supra note 232, Component 3, Project Appraisal Document,
273 The Election Laws Amendment Act, 2021.
274 The government had released an updated national identity policy which required individuals to link their NIN to SIM cards in December 2020, there has been a general hesitation by Nigerians, who see the move as inimical to their interests and wellbeing. The deadline for this NIN– SIM linkage has thus been postponed six times, with the sixth postponement coming in July 2021; see Avang Macdonald, "Nigeria's Move to Link Digital Identity Numbers to SIM Cards Sparks Lawsuit", Biometric Update, 2 February 2021,biometricupdate.com.
275 "Digital Identity in Nigeria ", Centre for Internet Society and Research ICT Africa, 2021, digitalid.design for more.
276 David P. Dolowitz and David Marsh, "Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making ", Governance, 17 December 2000.
277 David P. Dolowitz and David Marsh, "Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making ", Governance, 17 December 2000.
278 Barnett, M. and M Finnemore . Rules for the World: International Organizations in Global Politics. (London: Cornell University Press, 2004).
279 Refer to pages 31-35.
280 Refer to pages 50-57.
281 Kollman, K. "European Institutions, Transnational Networks a nd National Same-s ex Unions Policy: When Soft Law Hits Harder", Contemporary Politics 15, no. 1 (2009): 37–53.
282 Barnett, M. and M. Finnemore. Rules for the World: International Organizations in Global P olitics (London: Cornell University Press, 2004).
283 Refer to page 49.
284 "Research", Identification for Development, The World Bank, id4d.worldbank.org

Credits for Unsplash images:

Pg 2 - Ovinuchi Ejiohuo
Pg 4 - Giulia Lorenzon
Pg 10 - Udayaditya Barua
Pg 22 - Photos by Beks
Pg 45 - Nupo Deyon Daniel
Pg 46 - Olumide Bamgbelu
Pg 49 - Ron Dauphin


PRIVACY
INTERNATIONAL


THE
CENTRE
FOR
internet
& society